7TH EDITION

IT GOVERNANCE

An International Guide to Data Security and ISO27001/ISO27002

ALAN CALDER
STEVE WATKINS

KoganPage

IT Governance

IT Governance

An international guide to data security and ISO27001/ISO27002

SEVENTH EDITION

Alan Calder
Steve Watkins

Publisher's note
Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and authors cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or either of the authors.

First published in Great Britain and the United States in 2002 by Kogan Page Limited

Second edition 2003
Third edition 2005
Fourth edition 2008
Fifth edition 2012
Sixth edition 2015
Seventh edition 2020

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licences issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned addresses:

2nd Floor, 45 Gee Street
London
EC1V 3RS
United Kingdom
www.koganpage.com

122 W 27th St, 10th Floor
New York, NY 10001
USA

4737/23 Ansari Road
Daryaganj
New Delhi 110002
India

© Alan Calder and Steve Watkins, 2002, 2003, 2005, 2008, 2012, 2015, 2020

The right of Alan Calder and Steve Watkins to be identified as the author of this work has been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

ISBNs
Hardback 978 1 7896 6030 2
Paperback 978 0 7494 9695 1
Ebook 978 0 7494 9696 8

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

A CIP record for this book is available from the Library of Congress.

Typeset by Hong Kong FIVE Workshop
Print production managed by Jellyfish
Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY

CONTENTS

About the author xi

Introduction 1

1 Why is information security necessary? 9

The nature of information security threats 10
Information insecurity 12
Impacts of information security threats 13
Cybercrime 14
Cyberwar 16
Advanced persistent threat 17
Future risks 17
Legislation 20
Benefits of an information security management system 22

2 The Corporate Governance Code, the FRC Risk Guidance and Sarbanes–Oxley 23

The Combined Code 23
The Turnbull Report 24
The Corporate Governance Code 25
Sarbanes–Oxley 29
Enterprise risk management 31
Regulatory compliance 33
IT governance 34

3 ISO27001 37

Benefits of certification 37
The history of ISO27001 and ISO27002 38
The ISO/IEC 27000 series of standards 40
Use of the standard 41
ISO/IEC 27002 42
Continual improvement, Plan–Do–Check–Act, and process approach 43

Structured approach to implementation 44
Management system integration 47
Documentation 48
Continual improvement and metrics 53

4 Organizing information security 55

Internal organization 56
Management review 58
The information security manager 59
The cross-functional management forum 61
The ISO27001 project group 62
Specialist information security advice 68
Segregation of duties 70
Contact with special interest groups 71
Contact with authorities 73
Information security in project management 73
Independent review of information security 74
Summary 75

5 Information security policy and scope 77

Context of the organization 77
Information security policy 78
A policy statement 85
Costs and the monitoring of progress 86

6 The risk assessment and Statement of Applicability 89

Establishing security requirements 89
Risks, impacts and risk management 89
Cyber Essentials 99
Selection of controls and Statement of Applicability 106
Statement of Applicability Example 108
Gap analysis 109
Risk assessment tools 110
Risk treatment plan 111
Measures of effectiveness 112

7 Mobile devices 115

Mobile devices and teleworking 115
Teleworking 118

8 Human resources security 121

Job descriptions and competency requirements 121
Screening 123
Terms and conditions of employment 126
During employment 128
Disciplinary process 134
Termination or change of employment 135

9 Asset management 139

Asset owners 139
Inventory 140
Acceptable use of assets 143
Information classification 144
Unified classification markings 146
Government classification markings 148
Information lifecycle 149
Information labelling and handling 150
Non-disclosure agreements and trusted partners 155

10 Media handling 157

Physical media in transit 159

11 Access control 161

Hackers 161
Hacker techniques 162
System configuration 166
Access control policy 167
Network Access Control 169

12 User access management 179

User access provisioning 184

13 System and application access control 191

Secure log-on procedures 192
Password management system 193
Use of privileged utility programs 194
Access control to program source code 195

14 Cryptography 197
Encryption 198
Public key infrastructure 199
Digital signatures 200
Non-repudiation services 201
Key management 202

15 Physical and environmental security 205
Secure areas 205
Delivery and loading areas 214

16 Equipment security 217
Equipment siting and protection 217
Supporting utilities 220
Cabling security 222
Equipment maintenance 223
Removal of assets 224
Security of equipment and assets off-premises 224
Secure disposal or reuse of equipment 225
Clear desk and clear screen policy 227

17 Operations security 229
Documented operating procedures 229
Change management 231
Separation of development, testing and operational environments 233
Back-up 234

18 Controls against malicious software (malware) 239
Viruses, worms, Trojans and rootkits 239
Spyware 241
Anti-malware software 241
Hoax messages and Ransomware 243
Phishing and pharming 244
Anti-malware controls 245
Airborne viruses 248

Technical vulnerability management 250
Information Systems Audits 252

19 Communications management 253

Network security management 253

20 Exchanges of information 259

Information transfer policies and procedures 259
Agreements on information transfers 262
E-mail and social media 263
Security risks in e-mail 264
Spam 266
Misuse of the internet 266
Internet acceptable use policy 269
Social media 271

21 System acquisition, development and maintenance 273

Security requirements analysis and specification 273
Securing application services on public networks 274
E-commerce issues 275
Security technologies 278
Server security 281
Server virtualization 282
Protecting application services transactions 283

22 Development and support processes 285

Secure development policy 285
Secure systems engineering principles 289
Secure development environment 289
Security and acceptance testing 290

23 Supplier relationships 295

Information security policy for supplier relationships 295
Addressing security within supplier agreements 297
ICT supply chain 299
Monitoring and review of supplier services 301
Managing changes to supplier services 302

24 Monitoring and information security incident management 305

Logging and monitoring 305
Information security events and incidents 310
Incident management – responsibilities and procedures 310
Reporting information security events 313
Reporting software malfunctions 316
Assessment of and decision on information security events 318
Response to information security incidents 318
Legal admissibility 321

25 Business and information security continuity management 323

ISO22301 323
The business continuity management process 324
Business continuity and risk assessment 325
Developing and implementing continuity plans 327
Business continuity planning framework 328
Testing, maintaining and reassessing business continuity plans 332
Information security continuity 335

26 Compliance 339

Identification of applicable legislation 340
Intellectual property rights 353
Protection of organizational records 358
Privacy and protection of personally identifiable information 359
Regulation of cryptographic controls 361
Compliance with security policies and standards 361
Information systems audit considerations 364

27 The ISO27001 audit 365

Selection of auditors 365
Initial audit 367
Preparation for audit 368
Terminology 371

Appendix 1: Useful websites 373
Appendix 2: Further reading 379
Index 385

ABOUT THE AUTHORS

ALAN CALDER

Alan Calder founded IT Governance Limited in 2002 and began working full time for the company in 2007. He is now Group CEO of GRC International Group PLC, the AIM-listed company that owns IT Governance Ltd. Prior to this, Alan had a number of roles including CEO of Business Link London City Partners from 1995 to 1998 (a government agency focused on helping growing businesses to develop), CEO of Focus Central London from 1998 to 2001 (a training and enterprise council), CEO of Wide Learning from 2001 to 2003 (a supplier of e-learning) and the Outsourced Training Company (2005). Alan was also chairman of CEME (a public private sector skills partnership) from 2006 to 2011.

Alan is an acknowledged international cyber security guru and a leading author on information security and IT governance issues. He has been involved in the development of a wide range of information security management training courses that have been accredited by the International Board for IT Governance Qualifications (IBITGQ). Alan has consulted for clients in the UK and abroad, and is a regular media commentator and speaker.

STEVE WATKINS

Steve is an executive director at GRC International Group PLC. He is a contracted technical assessor for UKAS, advising on its assessments of certification bodies offering ISMS/ISO 27001 and ITSMS/ISO 20000-1 accredited certification, and also undertakes information security assessments of forensic science laboratories seeking accreditation to the Forensic Science Regulator's codes of practice and conduct.

He is a member of ISO/IEC JTC 1/SC 27, the international technical committee responsible for information security, cyber security and privacy standards, and chairs the UK National Standards Body's technical committee IST/33 (Information technology – Security techniques) that mirrors it. Steve is also involved with technical committees: RM/1 (risk management) and RM/1/-/3 (responsible for BS 31111, providing guidance for boards and senior management on cyber risk and resilience); IST/060/02 (IT service management) and IDT/001/0-/04 (data protection).

Introduction

This book on IT governance is a key resource for forward-looking executives and managers in 21st-century organizations of all sizes. There are six reasons for this:

1. The development of IT governance, which recognizes the 'information economy'-driven convergence between business management and IT management, makes it essential for executives and managers at all levels in organizations of all sizes to understand how decisions about information technology in the organization should be made and monitored and, in particular, how information security risks are best dealt with.
2. Risk management is a big issue. In the United Kingdom, the FRC's Risk Guidance (formerly the Turnbull Guidance on internal control) gives directors of Stock Exchange-listed companies a clear responsibility to act on IT governance, on the effective management of risk in IT projects and on computer security. The US Sarbanes–Oxley Act places a similar expectation on directors of all US listed companies. Banks and financial sector organizations are subject to the requirements of the Bank of International Settlements (BIS) and the Basel 2/3 frameworks, particularly around operational risk – which absolutely includes information and IT risk. Information security and the challenge of delivering IT projects on time, to specification and to budget also affect private- and public-sector organizations throughout the world.
3. Particularly post-GDPR, information-related legislation and regulation are increasingly important to all organizations. Data protection, privacy and breach regulations, computer misuse and regulations around investigatory powers are part of a complex and often competing range of requirements to which directors must respond. There is, increasingly, the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide.

4 As the intellectual capital value of 'information economy' organizations increases, their commercial viability and profitability – as well as their share price – increasingly depend on the security, confidentiality and integrity of their information and information assets.

5 The dramatic growth and scale of the 'information economy' have created new, global threats and vulnerabilities for all organizations, particularly in cyberspace.

6 The world's first, and only, standard for information security management is now at the heart of a globally recognized framework for information security and assurance. As part of the series of ISO/IEC 27000 standards, the key standard, ISO/IEC 27001, has been updated to contain latest international best practice, with which, increasingly, businesses are asking their suppliers to conform. Compliance with the standard should enable company directors to demonstrate a proper response – to customers as well as to regulatory and judicial authorities – to all the challenges identified above.

The information economy

Faced with the emergence and speed of growth in the information economy, organizations have an urgent need to adopt IT governance best practice. The main drivers of the information economy are:

- the ongoing globalization of markets, products and resourcing (including 'offshoring' and 'nearshoring');
- electronic information and knowledge intensity;
- the geometric increase in the level of electronic networking and connectivity.

The key characteristics of the global information economy, which affect all organizations, are as follows:

- Unlike the industrial economy, information and knowledge are not depleting resources that have to be rationed and protected.
- Protecting knowledge is less obviously beneficial than previously: sharing knowledge actually drives innovation, and innovation drives competitiveness.
- The effect of geographic location is diminished; virtual and cloud-based organizations operate around the clock in virtual marketplaces that have no geographic boundaries.

- As knowledge shifts to low-tax, low-regulation environments, laws and taxes are increasingly difficult to apply on a solely national basis.
- Knowledge-enhanced products command price premiums.
- Captured, indexed and accessible knowledge has greater intrinsic value than knowledge that goes home at the end of every day.
- Intellectual capital is an increasingly significant part of shareholder value in every organization.

The challenges, demands and risks faced by organizations operating in this information-rich and technologically intensive environment require a proper response. In the corporate governance climate of the early 21st century, with its growing demand for shareholder rights, corporate transparency and board accountability, this response must be a governance one.

What is IT governance?

The Organization for Economic Co-operation and Development (OECD), in its *Principles of Corporate Governance* (1999), first formally defined 'corporate governance' as 'the system by which business corporations are directed and controlled'. Every country in the OECD is evolving – at a different speed – its own corporate governance regime, reflecting its own culture and requirements. Within its overall approach to corporate governance, every organization has to determine how it will govern the information, information assets and information technology on which its business model and business strategy rely. This need has led to the emergence of IT governance as a specific – and pervasively important – component of an organization's total governance posture.

We define IT governance as 'the framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organization's information systems support and enable the achievement of its strategies and objectives'.

There are five specific drivers for organizations to adopt IT governance strategies:

- the requirements (in the United Kingdom) of the Corporate Governance Code and the Risk Guidance; for US-listed companies, Sarbanes–Oxley; for banks and financial institutions, BIS and Basel 2/3; and for businesses everywhere, the requirements of their national corporate governance regimes;

- the increasing intellectual capital value that the organization has at risk;
- the need to align technology projects with strategic organizational goals and to ensure that they deliver planned value;
- the proliferation of (increasingly complex) threats to information and information security, particularly in cyber space, with consequent potential impacts on corporate reputation, revenue and profitability;
- the increase in the compliance requirements of (increasingly conflicting and punitive) information- and privacy-related regulation, particularly the EU GDPR and regulations inspired by it.

There are two fundamental components of effective management of risk in information and information technology. The first relates to an organization's strategic deployment of information technology in order to achieve its business goals. IT projects often represent significant investments of financial and managerial resources. Shareholders' interest in the effectiveness of such deployment should be reflected in the transparency with which they are planned, managed and measured, and the way in which risks are assessed and controlled. The second component is the way in which the risks associated with information assets themselves are managed.

Clearly, well-managed information technology is a business enabler. All directors, executives and managers, at every level in any organization of any size, need to understand how to ensure that their investments in information and information technology enable the business. Every deployment of information technology brings with it immediate risks to the organization, and therefore every director or executive who deploys, or manager who makes any use of, information technology needs to understand these risks and the steps that should be taken to counter them. This book deals with IT governance from the perspective of the director or business manager, rather than from that of the IT specialist. It also deals primarily with the strategic and operational aspects of information security.

Information security

The proliferation of increasingly complex, sophisticated and global threats to information security, in combination with the compliance requirements of a flood of computer- and privacy-related regulation around the world, is driving organizations to take a more strategic view of information security.

It has become clear that hardware-, software- and/or vendor-driven solutions to individual information security challenges are, on their own, dangerously inadequate.

While most organizations believe that their information systems are secure, the brutal reality is that they are not. Not only is it extremely difficult for an organization to operate in today's world without effective information security, but poorly secured organizations have become risks to their more responsible associates. The extent and value of electronic data are continuing to grow exponentially. The exposure of businesses and individuals to data misappropriation (particularly in electronic format) or destruction is also growing very quickly. Ultimately, consumer confidence in dealing across the web depends on how secure consumers believe their personal data are. Cyber security, for this reason, matters to any business with any form of web strategy (and any business without a web strategy is unlikely to be around in the long term), from simple business-to-consumer (b2c) or business-to-business (b2b) e-commerce propositions through enterprise resource planning (ERP) systems to the use of e-mail, social media, mobile devices, Cloud applications and web services. It matters, too, to any organization that depends on computers for its day-to-day existence or that may be subject (as are all organizations) to the provisions of data protection legislation.

Newspapers and business or sector magazines are full of stories about criminal hackers, viruses, online fraud, cyber crime and loss of personal data. These are just the public tip of the data insecurity iceberg. There is growing evidence of substantial financial losses amongst inadequately secured businesses and a number of instances where businesses have failed to survive a major disruption of their data and operating systems. All businesses now suffer low-level, daily disruption of normal operations as a result of inadequate security.

Many people also experience the frustration of trying to buy something online, only for the screen to give some variant of the message 'server not available'. Many more, working with computers in their daily lives, have experienced (once too) many times a local network failure or outage that interrupts their work. With the increasing pervasiveness of computers, and as hardware/software computing packages become ever more powerful and complex, so the opportunity for data and data systems to be compromised or corrupted (knowingly or otherwise) will increase.

Information security management systems (ISMSs) in the vast majority of organizations are, in real terms, non-existent, and even where systems have

been designed and implemented, they are usually inadequate. In simple terms, larger organizations tend to operate their security functions in vertically segregated silos with little or no coordination. This structural weakness means that most organizations have significant vulnerabilities that can be exploited deliberately or that simply open them up to disaster.

For instance, while the corporate lawyers will tackle all the legal issues (nondisclosure agreements, patents, contracts, etc), they will have little involvement with the data security issues faced on the organizational perimeter. On the organizational perimeter, those dealing with physical security concentrate almost exclusively on physical assets, such as gates or doors, security guards and burglar alarms. They have little appreciation of, or impact upon, the 'cyber' perimeter. The IT managers, responsible for the cyber perimeter, may be good at ensuring that everyone has a strong password and that there is internet connectivity, that the organization is able to respond to malware threats, and that key partners, customers and suppliers are able to deal electronically with the organization, but they almost universally lack the training, experience or exposure adequately to address the strategic threat to the information assets of the organization as a whole. There are many organizations in which the IT managers subjectively set and implement security policy for the organization on the basis of their own risk assessment, past experiences and interests, but with little regard for the real business needs or strategic objectives of the organization.

Information security is a complex issue and deals with the confidentiality, integrity and availability of data. IT governance is even more complex, and in information security terms one has to think in terms of the whole enterprise, the entire organization, which includes all the possible combinations of physical and cyber assets, all the possible combinations of intranets, extranets and internets, and which might include an extended network of business partners, vendors, customers and others. This handbook guides the interested manager through this maze of issues, through the process of implementing internationally recognized best practice in information security, as captured in ISO/IEC 27002:2013 and, finally, achieving certification to ISO/IEC 27001:2013, the world's formal, public, international standard for effective information security management.

The ISMS standard is not geographically limited (eg to the United Kingdom, or Japan or the United States), nor is it restricted to a specific sector (eg the Department of Defence or the software industry), nor is it restricted to a specific product (such as an ERP system, or Software as a Service). This book covers many aspects of data security, providing sufficient

information for the reader to understand the major data security issues and what to do about them – and, above all, what steps and systems are necessary for the achievement of independent certification of the organization's ISMS to ISO27001.

This book is of particular benefit to board members, directors, executives, owners and managers of any business or organization that depends on information, that uses computers on a regular basis, that is responsible for personal data or that has an internet aspect to its strategy. It can equally apply to any organization that relies on the confidentiality, integrity and availability of its data. It is directed at readers who either have no prior understanding of data security or whose understanding is limited in interest, scope or depth. It is not written for technology or security specialists, whose knowledge of specific issues should always be sought by the concerned owner, director or manager. While it deals with technology issues, it is not a technological handbook.

Information security is a key component of IT governance. As information technology and information itself become more and more the strategic enablers of organizational activity, so the effective management of both and information assets becomes a critical strategic concern for boards of directors. This book will enable directors and business managers in organizations and enterprises of all sizes to ensure that their IT security strategies are coordinated, coherent, comprehensive and cost-effective, and meet their specific organizational or business needs. While the book is written initially for UK organizations, its lessons are relevant internationally, as computers and data threats are internationally similar. Again, while the book is written primarily with a Microsoft environment in mind (reflecting the penetration of the Microsoft suite of products into corporate environments), its principles apply to all hardware and software environments. ISO/IEC 27001 is, itself, system agnostic.

The hard copy of this book provides detailed advice and guidance on the development and implementation of an ISMS that will meet the ISO27001 specification. The IT Governance website (www.itgovernancepublishing.co.uk/category/toolkits-information-security-iso27001 (archived at https://perma.cc/7FED-RY3Y)) carries a series of ISO27001 Documentation Toolkits. Use of the templates within these toolkits, which are not industry or jurisdiction specific but which do integrate absolutely with the advice in this book, can speed knowledge acquisition and ensure that your process development is comprehensive and systematic.

Organizations should always ensure that any processes they implement are appropriate and tailored for their own environment. There are four reasons for this:

- Policies, processes and procedures should always reflect the style, and the culture, of the organization that is going to use them. This will help their acceptance within the organization.
- The processes and procedures that are adopted should reflect the risk assessment carried out by the organization's specialist security adviser. While some risks are common to many organizations, the approach to controlling them should be appropriate to, and cost-effective for, the individual organization and its individual objectives and operating environment.
- It is important that the organization understands, in detail, its policies, processes and procedures. It will have to review them after any significant security incident and at least once a year. The best way to understand them thoroughly is through the detailed drafting process.
- Most importantly, the threats to an organization's information security are evolving as fast as the information technology that supports it. It is essential that security processes and procedures are completely up to date, that they reflect current risks and that, in particular, current technological advice is taken, to build on the substantial groundwork laid in this book.

This book will certainly provide enough information to make the drafting of detailed procedures quite straightforward. Where it is useful (particularly in generic areas like e-mail controls, data protection, etc), there are pointers as to how procedures should be drafted. Information is the very lifeblood of most organizations today and its security ought to be approached professionally and thoroughly.

Finally, it should be noted that ISO27001 is a service assurance scheme, not a product badge or cast-iron guarantee. Achieving ISO27001 certification does not of itself prove that the organization has a completely secure information system; it is merely an indicator, particularly to third parties, that the objective of achieving appropriate security is being effectively pursued. Information security is, in the terms of the cliché, a journey, not a destination.

1

Why is information security necessary?

An information security management system (ISMS) is necessary because the threats to the availability, integrity and confidentiality of the organization's information are great, and always increasing. Any prudent householder whose house was built on the shores of a tidal river would, when facing the risk of floods, take urgent steps to improve the defences of the house against the water. It would clearly be insufficient just to block up the front gate, because the water would get in everywhere and anywhere it could. In fact, the only prudent action would be to block every single possible channel through which floodwaters might enter and then to try to build the walls even higher, in case the floods were even worse than expected.

So it is with the threats to organizational information, which are now reaching tidal proportions. All organizations possess information, or data, that is either critical or sensitive. Information is widely regarded as the lifeblood of modern business. Advanced Persistent Threat (APT) is the description applied to the cyber activities of sophisticated criminals and state-level entities, targeted on large corporations and foreign governments, with the objective of stealing information or compromising information systems. Cyber attacks are, initially, automated and indiscriminate – any organization with an internet presence will be scanned and potentially targeted.

Not surprisingly, the PricewaterhouseCoopers (PwC) Global State of Information Security Survey 2018 said that 'most organizations realize that cybersecurity has become a persistent, all-encompassing business risk'. This is because the business use of technology is continuing to evolve rapidly, as organizations move into cloud computing and exploit social networks. Wireless networking, Voice over IP (VoIP) and Software as a Service (SaaS)

have become mainstream. The increasingly digital and inter-connected supply chain increases the pressure on organizations to manage information and its security and confirms the growing dependence of UK business on information and information technology.

While it is clearly banal to state that today's organization depends for its very existence on its use of information and communications technology, it is apparently not yet self-evident to the vast majority of boards and business owners that their information is valuable to both competitors and criminals and that how well they protect their systems and information is existentially important.

There is no doubt that organizations are facing a flood of threats to their intellectual assets and to their critical and sensitive information. High-profile cyber attacks and data protection compliance failures have led to significant embarrassment and brand damage for organizations – in both the public and private sectors – all over the world.

In parallel with the evolution of information security threats, there has – across the world – been a thickening web of legislation and regulation that makes firms criminally liable, and in some instances makes directors personally accountable, for failing to implement and maintain appropriate risk control and information security measures. It is now blindingly obvious that organizations have to act to secure and protect their information assets.

'Information security', however, means different things to different people. To vendors of security products, it tends to be limited to the product(s) they sell. To many directors and managers, it tends to mean something they don't understand and that the CIO, CISO or IT manager has to put in place. To many users of IT equipment, it tends to mean unwanted restrictions on what they can do on their corporate PCs. These are all dangerously narrow views.

The nature of information security threats

Data or information is right at the heart of the modern organization. Its availability, integrity and confidentiality are fundamental to the long-term survival of any 21st-century organization; in survey after survey, 9 out of 10 organizations make this claim. Unless the organization takes a comprehensive and systematic approach to protecting the availability, integrity and confidentiality of its information, it will be vulnerable to a wide range of possible threats. These threats are not restricted to internet companies, to

e-commerce businesses, to organizations that use technology, to financial organizations or to organizations that have secret or confidential information. As we saw earlier, they affect all organizations, in all sectors of the economy, both public and private. They are a 'clear and present danger', and strategic responsibility for ensuring that the organization has appropriately defended its information assets cannot be abdicated or palmed off on the CIO, CIOS or head of IT.

In spite of surveys and reports which claim that boards and managers are paying more attention to security, the truth is that the risk to information is growing more quickly than boards are recognizing. The annual Verizon Data Breaches Report gathered data from 80,000 data breaches (which occurred in a 12-month period) across the world to conclude that 700 million compromised records were the cause of financial losses of some $400 million. Matters are worse in every subsequent year.

Information security threats come from both within and without an organization. The situation worsens every year, and cyber threats are likely to become more serious in future. Cyber activism is at least as serious a threat as is cyber crime, cyber war and cyber terrorism. Unprovoked external attacks and internal threats are equally serious. It is impossible to predict what attack might be made on any given information asset, or when, or how. The speed with which methods of attack evolve, and knowledge about them proliferates, makes it completely pointless to take action only against specific, identified threats. Only a comprehensive, systematic approach will deliver the level of information security that any organization really needs.

It is worth understanding the risks to which an organization with an inadequate ISMS exposes itself. These risks fall into three categories:

- damage to operations;
- damage to reputation;
- legal damage.

Damage in any one of these three categories can be measured by its impact on the organization's bottom line, both short and long term. While there is no single, comprehensive, global study of information risks or threats on which all countries and authorities rely, there are a number of surveys, reports and studies, in and across different countries and often with slightly differing objectives, that, between them, demonstrate the nature, scale, complexity and significance of these information security risks and the extent to which organizations, through their own complacency or through

the vulnerabilities in their hardware, software, and management systems, are vulnerable to these threats.

Information insecurity

Annual surveys point to a steadily worsening situation. The annual Verizon Data Breach Investigations Report, conducted with the US Secret Service, and which draws data from both the United States and internationally, regularly reports that:

- data breaches occur within all sorts of organizations;
- hundreds of millions of records are compromised every year;
- most breaches originate externally, a significant per cent internally, and more than a quarter were carried out by multiple agents.

The United Kingdom's annual Information Security Breaches Survey (ISBS), managed by PwC, looks at the state of information security across a representative sample of UK organizations. Key findings include:

- Almost all large organizations suffer data breaches, and often multiple breaches; large organizations tend to be specifically targeted by attackers.
- More than 50% of small organizations are breached; because they are not specifically targeted, they suffer fewer breaches every year.
- The average cost to a large organization of its worst breach is between £600k and £1.15 million.
- For a small organization, the range is between £65k and £115k.
- More than three-quarters of large respondents suffer from a malware or virus infection, often delivered via a phishing e-mail.
- More than half of large respondents suffer an external attack; quite often this is some form of denial of service attack, and less than a quarter are able to identify that their defences have actually been penetrated.
- The majority of organizations also suffer staff-related security breaches; one-third of the worst breaches are caused by inadvertent human error.

Surveys and data from other OECD economies suggest that a similar situation can be found across the world. Hackers, crackers, virus writers, spammers, phishers, pharmers, fraudsters and the whole menagerie of cyber-criminals

are increasingly adept at exploiting the vulnerabilities in organizations' software, hardware, networks and processes. As fraudsters, spam and virus writers, hackers and cyber criminals band together to mount integrated attacks on businesses and public sector organizations everywhere, the need for appropriate cyber security defences increases.

Often – but not always – information security is *in reality* seen only as an issue for the IT department, which it clearly isn't. Good information security management is about organizations understanding the risks and threats they face and the vulnerabilities in their current computer processing facilities. It is about putting in place common-sense procedures to minimize the risks and about educating all the employees about their responsibilities. Most importantly, it is about ensuring that the policy on information security management has the commitment of senior managers. It is only when these procedural and management issues are addressed that organizations can decide on what security technologies they need.

Roughly one-seventh of businesses are still spending less than 1 per cent of their IT budget on information security; although the average company is spending just under 4 per cent, the benchmark against which their expenditure should be compared is closer to the 13 per cent average of organizations where managers genuinely care about information security. That less than half of all businesses ever estimate the return on their information security investment may be part of the problem; certainly, until business takes its IT governance responsibilities seriously, the information security situation will continue to worsen.

Impacts of information security threats

As indicated above, information security breaches affect business operations, reputation and legal standing. Business disruption is the most serious impact, with roughly two-thirds of UK breaches leading to disruption of operations, with consequent impacts on customer service and business efficiency. As well as business disruption, organizations face incident response costs that include response and remediation costs (responding to, fixing and cleaning up after a security breach), direct financial loss (loss of assets, regulatory fines, compensation payments), indirect financial loss (through leakage of confidential information or intellectual property, revenue leakage), and reputation damage, with successful hack attacks and data losses both attracting increasing media attention.

There is a wide range of information available about the nature and average cost of a breach. The annual Verizon DBIR gathers information from 61 countries and multiple industry sectors in order to conclude that no industry is immune from data breaches. In 60 per cent of cases, attackers are able to compromise targets 'within minutes'; it still takes longer to detect the compromise than it does to complete the attack. Verison's forecast average financial loss per breach of 1,000 records is between $52,000 and $87,000. Most importantly, they conclude that the consistently most significant factor in quantifying the cost of loss for an organization is not the nature of the breach, but the number of records compromised.

The various components of that financial loss include discovery, investigation, response, remediation, customer notification costs, legal fees, regulatory breach notification costs, and increased operational, marketing and PR costs.

As the Target (a large US retailer) breach, in the USA just before Thanksgiving back in 2013, proved, damage to corporate reputation, shareholder class actions and straightforward loss of customers and the fall in net revenue arising from a successful breach can have a far more significant impact on the future performance of the organization – and, increasingly, on the continued employment and future careers of the directors at the helm of the organization when the breach occurred.

Cybercrime

The US State of Cybercrime Survey (conducted by CSO Magazine, the US Secret Service, the CERT Division of the Software Engineering Institute, and Price Waterhouse Cooper) spoke to 557 organizations about their experience in the previous 12 months. Thirty-two per cent of respondents said that damage from insider attacks was more severe than that from outsiders; 76 per cent of incidents involved theft or compromise of confidential records. Thirty-seven per cent of cybercrimes were not prosecuted because the culprits could not be identified and, for 36 per cent, the evidence was inadequate to support a prosecution.

In reality, many information security incidents are actually crimes. The UK Computer Misuse Act, for instance, makes it an offence for anyone to access a computer without authorization, to modify the contents of a

computer without authorization or to facilitate (allow) such activity to take place. It identified sanctions for such activity, including fines and imprisonment. Other countries have taken similar action to identify and create offences that should enable law enforcement bodies to act to deal with computer misuse. Increasingly, this type of illegal activity is known as 'cybercrime'.

The Council of Europe Cybercrime Convention, the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks, was signed in November 2001. The United States finally ratified the Cybercrime Convention in 2006 and joined with effect from 1 January 2007. The Cybercrime Convention was designed to protect citizens against computer hacking and internet fraud, and to deal with crimes involving electronic evidence, including child sexual exploitation, organized crime and terrorism. Parties to the convention commit to effective and compatible laws and tools to fight cybercrime, and to cooperating to investigate and prosecute these crimes. They are not succeeding in this aim.

Europol, the European police agency, publishes the Internet Organized Crime Threat Assessment (iOCTA). iOCTA 2014 said that current trends suggest considerable increases in the scope, sophistication, number and types of attacks, number of victims and economic damage from organized crime on the Internet. The Crime-as-a-Service (CaaS) business model drives the digital underground economy by providing a wide range of commercial services that facilitate almost any type of cybercrime. Criminals are freely able to procure such services, such as the rental of botnets, denial-of-service attacks, malware development, data theft and password cracking, to commit crimes themselves. This has facilitated a move by traditional organized crime groups (OCGs) into cybercrime areas. The financial gain that cybercrime experts have from offering these services stimulates the commercialization of cybercrime as well as its innovation and further sophistication. Legitimate privacy networks are also of primary interest to criminals that abuse such anonymity on a massive scale for illicit online trade in drugs, weapons, stolen goods, forged IDs and child sexual exploitation.

The internet is, in other words, digitally dangerous. Organizations must take appropriate steps to protect themselves against criminal activity – both internal and external – in just the same way as they take steps to protect themselves in the physical world.

Cyberwar

Cybercrime is a serious issue but, in the longer run, may be a lesser danger to organizations than the effects of what is called 'cyberwar'. It is believed that every significant terrorist or criminal organization has cyber-capabilities and has become very sophisticated in its ability to plan and execute digital attacks. More significantly, many nation states now see cyberwar as an alternative – or an essential precursor to – traditional warfare.

Eliza Manningham-Buller, the then director-general of the UK security service MI5, said this at the 2004 CBI annual conference:

> A narrow definition of corporate security including the threats of crime and fraud should be widened to include terrorism and the threat of electronic attack. In the same way that health and safety and compliance have become part of the business agenda, so should a broad understanding of security, and considering it should be an integral and permanent part of your planning and statements of internal control; do not allow it to be left to specialists. Ask them to report to you what they are doing to identify and protect your key assets, including your people.

A decade later, Sir Ian Lobban said much the same thing in an open letter to CEOs and Chairs of FTSE 350 companies, encouraging them to undertake a 'cyber health check' after a KPMG security survey found that all of them were leaking data, such as employee usernames, e-mail addresses and sensitive internal file location information online.

Certainly, businesses appear to have got this message, with 97 per cent of them claiming to be concerned at board level about cyberwar. They should be. More than 400 million computers are linked to the internet; many of them are vulnerable to indiscriminate cyber-attack. The critical infrastructure of the First World is subject to the threat of cyber-assaults ranging from defacing websites to undermining critical national infrastructure.

A growing number of countries are at last putting cyber security strategies in place. The UK government's 2015 national security strategy recognized cyber risk as a Tier 4 national security risk and its national cyber security strategy has the objective of making the UK one of the most secure places in the world to live and work online. The EU's 2013 cyber security strategy ('An Open, Safe and Secure Cyberspace') has similar objectives.

While organizations that are part of the Critical National Infrastructure (CNI) clearly have a significant role to play in preparing to defend their national cyberspace against cyberattack, all organizations should take

appropriate steps to defend themselves from being caught in the digital crossfire.

Advanced persistent threat

The term advanced persistent threat (APT) usually refers to a national government – or state-level entity that has the capacity and the intent to persistently and effectively target – in cyberspace – another entity that it wishes to disrupt or otherwise compromise. While cyberspace is the most common theatre of attack, other vectors include social engineering, infected media and malware and supply chain compromise. Attackers usually have the resources, competence and available time to focus on attacking one or more specific entities. The Stuxnet worm is an example of one such attack, but there are many others. For most large organizations, the critical consideration is not whether or not they have been targeted (they will have been), but whether or not they have been able to identify and neutralize the intrusion.

Future risks

There are a number of trends that lie behind these increases in threats to computer-based information security, which when taken together suggest that things will continue to get worse, not better:

1 The use of distributed computing is increasing. Computing power has migrated from centralized mainframe computers and data processing centres to a distributed network of desktop computers, laptop computers, microcomputers, and mobile devices, and this makes information security much more difficult to ensure.

2 There is an unstoppable trend towards mobile computing. The use of laptop computers, personal digital assistants (PDAs), mobile and smartphones, digital cameras, portable projectors, MP3 players and iPads has made working from home and while travelling relatively straightforward, with the result that network perimeters have become increasingly porous. This means that the number of remote access points to networks, and the number of easily accessible endpoint devices, have increased dramatically, and this has increased the opportunities for those who wish to break into networks and steal or corrupt information.

3 There has been a dramatic growth in the use of the internet for business and social media communication, and the development of wireless, voice over IP (VoIP) and broadband technologies is driving this even further. The internet provides an effective, immediate and powerful method for organizations to communicate on all sorts of issues. This exposes all these organizations to the security risks that go with connection to the internet:
   - The internet is really just a backbone connection that enables every computer in the world to connect to every other computer. This gives criminals a direct means of reaching any and every organization that is connected to the internet.
   - The internet is inherently a public space. It is accessible by anyone from anywhere and consists of the millions of connections, some permanent and some temporary, that come about because of this. It has no built-in security and no built-in protection for confidential or private information.
   - The internet (together with cellular telephony) is also, in effect, a worldwide medium for criminals and hackers to communicate with one another, to share the latest tricks and techniques and to work together on interesting projects.
   - Better hacker tools are available every day, on hacker websites that, themselves, proliferate. These tools are improved regularly and, increasingly, less and less technologically proficient criminals – and computer-literate terrorists – are thus enabled to cause more and more damage to target networks and systems.
   - Increasingly, hackers, virus writers and spam operators are cooperating to find ways of spreading more spam – not just because it's fun, but because there's a lot of money to be made out of the direct e-mail marketing of dodgy products. Phishing, pharming and other internet fraud activity will continue evolving and are likely to become an ever bigger problem.
4 This is leading, inevitably, to an increase in 'blended' threats, which can only be countered with a combination of technologies and processes.
5 Increasingly sophisticated technology defences, particularly around user authorization and authentication, will drive an increase in 'social engineering'-derived hacker attacks.
6 Computer literacy is becoming more widespread. While most people today have computer skills, the next generation are growing up with a

level of familiarity with computers that will enable them to develop and deploy an entirely new range of threats. Instant messaging is an example of a new technology that was better than e-mail in that it was faster and more immediate, but has many more security vulnerabilities than e-mail. We will see many more such technologies emerging.

7 Wireless technology – whether Wi-Fi or Bluetooth – makes information and the internet available cheaply and easily from virtually anywhere, thereby potentially reducing the perceived value and importance of information and certainly exposing confidential and sensitive information more and more to casual access.

8 The falling price of computers and mobile devices has brought computing within most people's reach. The result is that most people now have enough computer experience to pose a threat to an organization if they are prepared to apply themselves just a little bit to take advantage of the opportunities identified above.

What do these trends, and all these statistics from so many organizations in so many countries (and information security professionals would argue that, as most organizations don't yet know that their defences have already been breached, the statistics are only the tip of the iceberg), mean in real terms to individual organizations? In simple, brutal terms, they mean that:

- No organization is immune.
- Every organization, at some time, will suffer one or more of the disruptions, abuses or attacks identified in these pages.
- Businesses will be disrupted. Downtime in business-critical systems such as enterprise resource planning (ERP) systems can be catastrophic for an organization. However quickly service is restored, there will be an unwanted and unnecessary cost in doing so. At other times, lost data may have to be painstakingly reconstructed and sometimes will be lost forever.
- Privacy will be violated. Organizations have to protect the personal information of employees and customers. If this privacy is violated, there may be legal action and penalties.
- Organizations will continue suffering direct financial loss. Protection in particular of commercial information and customers' credit card details is essential. Loss or theft of commercial information, ranging from business plans and customer contracts to intellectual property and product designs, and industrial know-how, can all cause long-term financial

damage to the victim organization. Computer fraud, conducted by staff with or without third-party involvement, has an immediate direct financial impact.

- Regulation and compliance requirements will increase. Regulators will increasingly legislate to force corporations to take appropriate information security action and that will drive up the cost and complexity of information security. Breaches will increasingly also trigger mandatory reporting requirements and lead to significant fines.
- Reputations will be damaged. Organizations that are unable to protect the privacy of information about staff and customers, and which consequently attract penalties and fines, will find their corporate credibility and business relationships severely damaged and their expensively developed brand and brand image dented.

The statistics are compelling. The threats are evident. No organization can afford to ignore the need for information security. The fact that the risks are so widespread and the sources of danger so diverse means that it is insufficient simply to implement an antivirus policy, or a business continuity policy, or any other standalone solution. A conclusion of the CBI Cybercrime Survey 2001 was that 'deployment of technologies such as firewalls may provide false levels of comfort unless organizations have performed a formal risk analysis and configured firewalls and security mechanisms to reflect their overall risk strategy'. Nothing has changed. It was clear from the UK's ISBS that there is a correlation between security expenditure and risk assessments. On average, those respondents that carried out a risk assessment spent 8 per cent of their IT budget on security. The average expenditure for those that did not was 5 per cent or less. It seems likely, therefore, that those that have not actually assessed their information security risks are also under-investing in their security.

The only sensible option is to carry out a thorough assessment of the risks facing the organization and then to adopt a comprehensive and systematic approach to information security that cost-effectively tackles those risks.

Legislation

Certainly, organizations can legally no longer ignore the issue. There is a growing number of laws that are relevant to information security. In the

United Kingdom, for instance, relevant laws include the Companies Act 2006; the Copyright, Designs and Patents Act 1988; the Computer Misuse Act 1990 (as updated by the Police and Justice Act 2006); and the Data Protection Act 2018.

The Data Protection Act 2018 (DPA) is perhaps the most high-profile of these recently passed laws; it implements the EU GDPR into UK legislation and requires organizations in both the public and the private sectors to implement data security measures to prevent unauthorized or unlawful processing (which includes storing) and accidental loss or damage to data pertaining to living individuals. Fines of up to 4 per cent of global turnover may be imposed by the Information Commissioner's Office for breaches of the DPA.

While these Acts apply to all UK-based organizations, Stock Exchange-listed companies are also expected to comply with the recommendations of the UK Corporate Governance Code and the Risk Guidance on effective controls. Crucially, these require directors to take a risk assessment-based approach to their management of the business and to consider all aspects of the business in doing so.

In the United States, most states now have data breach reporting laws, and sectoral regulation such as HIPAA, GLBA, FISMA and others impose strict requirements on organizations. While the United States still has no federal data protection legislation, California (CCPA) does. So do Canada (PIPEDA), Australia and other members of the Commonwealth. In the EU all countries are subject to the EU GDPR, the core of which is exactly the same in all member states. Emerging economies are also passing data protection and cyber security laws, recognizing that improved security is a prerequisite for competing in the data-rich developed world.

In parallel, PCI DSS, a private sector security standard, has emerged as a contractual requirement for organizations that accept payment cards and, interestingly, compliance with PCI DSS has been enshrined in law in some US states; the ICO, in the UK, has recognized its importance.

Directors of listed businesses, of public-sector organizations and of companies throughout their supply chains must be able to identify the steps that they have taken to protect the confidentiality, integrity and availability of the organization's information assets. In all these instances, the existence of a risk-based information security policy, implemented through an ISMS, is clear evidence that the organization has taken the necessary and appropriate steps.

Benefits of an information security management system

The benefits of adopting an externally certifiable ISMS are, therefore, clear:

- The directors of the organization will be able to demonstrate that they are complying with the relevant requirements of Sarbanes–Oxley, Basel 2/3, the FRC's Risk Guidance or with current international best practice in risk management with regard to information assets and security.
- The organization will be able to demonstrate, in the context of the array of relevant legislation, that it has taken appropriate compliance action, particularly with data protection legislation such as the GDPR.
- The organization will be able systematically to protect itself from the dangers and potential costs of computer misuse, cybercrime and the impacts of cyberwar.
- The organization will be able to improve its credibility with staff, customers and partner organizations, and this improved credibility can have direct financial benefits through, for instance, improved sales. This competitive requirement is increasingly becoming a critical factor for organizations in winning new business from clients that are aware of the need for their suppliers to demonstrate they have implemented effective information security management measures.
- The organization will be able to make informed, practical decisions about what security technologies and solutions to deploy and thus to increase the value for money it gets from information security, to manage and control the costs of information security and to measure and improve its return on its information security investments.

2

The Corporate Governance Code, the FRC Risk Guidance and Sarbanes–Oxley

The Combined Code

The first version of the UK Combined Code, issued in 1998, replaced, combined and refined the earlier requirements of the Cadbury and Greenbury reports on corporate governance and directors' remuneration. It came into force for all listed companies for year-ends after December 1998. Since then, UK corporate governance has been on a 'comply or explain' basis; in other words, listed companies are expected to comply but are not statutorily required to do so. Simplistically, if they have good reason, they can choose not to comply with a particular provision of the Combined Code as long as they then explain, in their annual report, why that decision was taken. However, as the market nowadays punishes companies that choose not to comply, any decision about non-compliance is not expected to be taken lightly. (In actual fact, the requirements are a bit more complex than this.)

The Combined Code requirements were broadly similar to those of the earlier reports, but in one important respect – reporting on controls – there was a major and significant development in 1999, prior to the May 2010 revision of what is now formally the UK Corporate Governance Code. While the Cadbury Report had envisaged companies reporting on controls generally, the original guidance that was issued at that time to clarify those requirements permitted, and indeed encouraged, companies to restrict their review of controls, and the disclosures relating to that review, to financial controls.

This meant that potentially more important issues relating to *operational* control were left outside the reporting framework. The current version of the Corporate Governance Code was published in September 2014 and applies to companies listed on the main UK stock exchange (but not to AIM-listed companies). Principle C.2 of the Code says: 'The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.'

The Turnbull Report

The Turnbull Report – 'Internal Control: Guidance for directors on the Combined Code', published by the Internal Control Working Party of the Institute of Chartered Accountants in England and Wales – provided further guidance in 1999 as to how directors of listed companies should tackle this issue. After multiple revisions, it is now an FRC (published September 2014) publication formally titled 'Guidance on Risk Management, Internal Control, and Related Financial and Business Reporting'. It provides specific guidance on how to apply section C.2 of the Code, which deals with risk management and internal control and establishes the principle that: 'risk management and internal control should be incorporated within the company's normal management and governance processes, not treated as a separate compliance exercise.'

Paragraph 28 of the Risk Guidance states that a company's 'internal control system encompasses the policies, culture, organization, behaviours, processes, systems and other aspects of a company' that, taken together:

- Facilitate its effective and efficient operation by enabling it to assess current and emerging risks, respond appropriately to risks and and significant control failures and to safeguard its assets.
- Help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organization.
- Help ensure compliance with applicable laws and regulations.

Paragraph 29 recognizes that 'a company's system of risk management and internal control will include risk assessment, management or mitigation of

risks, including the use of control processes; *information and communications processes'*. Paragraph 33 is clear that, while risks may differ between companies, they 'may include financial, operational, reputational, behavioural, organizational, third party, or external risks'.

In short, the Risk Guidance makes it clear to the directors of public companies that their internal control systems have to address all forms of information as well as the systems on which it resides.

The Corporate Governance Code

Following the work of the Smith and Higgs committees, the Combined Code was revised and reissued on a regular basis, each time replacing the earlier versions. The most recent version was September 2014.

In section A.1, the UK Corporate Governance Code states that the 'board's role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enables risk to be assessed and managed'. Risk management, in other words, is a key responsibility of the board. The non-executive directors are required to 'satisfy themselves on the integrity of financial information and that financial controls and *systems of risk management are robust and defensible* [emphasis added]'.

Principle C.2 of the UK Corporate Governance Code deals with internal control. The board is required to maintain a sound system of internal control to safeguard shareholders' investments and the assets of the company. In practice, directors are required at least annually, to conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. 'The monitoring and review should cover all material controls, including financial, *operational and compliance controls* [emphasis added]'. The Code refers the reader to the Risk Guidance for details on how to apply this provision.

Copies of the UK Corporate Governance Code and Risk Guidance can both be obtained from the United Kingdom's Financial Reporting Council (FRC) or downloaded from www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code (archived at https://perma.cc/9F8Y-6E5P)

Paragraphs 24, 26 and 27 of the Risk Guidance provide an admirably brief and clear description of the principles of risk management and of the board's responsibility to set the policy around risk treatment, the executives

to implement it, and that of all staff to comply with the system of internal control. This sort of framework is often known as an enterprise risk management (ERM) framework, and an organization's ERM framework will reflect the overlap between regulatory risk management requirements as well as its specific internal control and information security management needs.

While listed companies are not legally required to comply with the provisions of the UK Corporate Governance Code, the FCA Listing Rules (LR.9.8.6 R et seq) require every Stock Exchange-listed (ie not Alternative Investment Market (AIM)-listed) company to include the following items in its annual report and accounts:

> 'a statement of how the listed company has applied the Main Principles set out in the Code, in a manner that would enable shareholders to evaluate how the principles have been applied;
>
> statement as to whether the listed company has:
>
> **a** complied throughout the accounting period with all relevant provisions set out in the Code; or
>
> **b** not complied throughout the accounting period with all relevant provisions set out in the Code and if so, setting out:
>
> **i** those provisions, if any, it has not complied with;
>
> **ii** in the case of provisions whose requirements are of a continuing nature, the period within which, if any, it did not comply with some or all of those provisions; and
>
> **iii** the company's reasons for non-compliance.'

There must also be conformation from the directors that they have carried out a robust assessment of the principal risks facing the company.

The company's auditors must verify statements made by the directors in respect of the board's compliance with the Code's provisions. In effect, compliance has become a fiduciary duty of boards of directors. This could mean that directors are held to be personally liable for any negative results of failing to apply the UK Corporate Governance Code or the Risk Guidance in a reasonable manner.

The UK Companies Act 2004 created a statutory duty for directors of companies, having made appropriate due and diligent inquiry, to make auditors aware of any factors that might be relevant to their assessment of a company's report and accounts, including all those statements within the

directors' report that auditors are required to comment on. This provision has been carried forward to the Companies Act 2006. This leaves no 'wiggle room' for directors; all important risk issues have to be identified and disclosed.

While the UK Corporate Governance Code is not, at first sight, relevant to any businesses other than those listed on the UK Stock Exchange, its impact is widely felt throughout the United Kingdom and through the national and international supply chains of UK-listed companies. This means that the FRC Risk Guidance will have an impact on all businesses in those supply chains, and all directors of them will need therefore to be aware of its requirements and implications. It has particular relevance to the management and security of data assets.

The UK government (through HM Treasury) adopted the principles of internal control set out by Turnbull and in 2004 published its 'Orange Book' (*Management of Risk – Principles and concepts*), in which it adapted Turnbull's recommendations to the public sector. All non-governmental organizations (NGOs) and non-departmental public bodies (NDPBs) are expected to conform to these requirements, and all government and government-controlled bodies were expected to ensure implementation and integration of the processes.

The key questions that directors of listed companies and 'Orange Book' public-sector organizations seek to answer in respect of their supply chains are the same questions that directors of companies in those supply chains therefore need to be able to answer for themselves. These questions (which are not meant to be exhaustive) now set out in Appendix C to the Risk Guidance and are quoted below. Key questions the board could ask include the following:

- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation and business probity issues.)
- Does the board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?
- Are information needs and related information systems reassessed as objectives and related risks change, or as reporting deficiencies are identified?

- Are there specific arrangements for management monitoring and reporting to the board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position.

The Risk Guidance does not specify which risks should be included in the scope of the board report and what can be left out. The Guidance simply says, in paragraph 24, that 'the board has responsibility for an organization's overall approach to risk management and internal control.' It goes on to stress that the board should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. Finally, it makes the point that the board is responsible for determining its risk appetite and for putting in place adequate processes for assuring itself that its risk management objectives are being achieved.

Given the absence of definitive guidance on what risks to include or exclude, the board of directors should seek to be as comprehensive as possible. This means that (among others, including health and safety, environment, employment legislation as well as more obvious strategic risks) information risk (covered in Chapter 1 of this book) must be considered, and therefore information security management will be critical to all organizations. Equally, in assessing risks to the organization, directors will have to assess the risks associated with their supply chains. Data interdependence is a characteristic of supply chains, and therefore risks to data security anywhere in the supply chain are a risk to the whole supply chain. Boards will have to assess these risks, the scale of which were indicated in Chapter 1, and implement appropriate control mechanisms to limit their potential impact.

It is clear that systems designed to meet the requirements of the FRC Risk Guidance should be integrated into the organization. This means that the necessary internal control systems should form part of the organizational culture and be part of the day-to-day management of the organization. They certainly should not be a separate structure designed solely for the purpose of complying with the Code, nor should they be introduced from outside the organization without there being real ownership within – and from the top of – the organization. Implementation does require the entire organization to embrace the principles of the Code; this can only happen if the process is taken sufficiently seriously for it to be embraced at board level and to be owned by the chairperson, CEO and the whole board.

Sarbanes–Oxley

The Sarbanes–Oxley Act of 2002 (SOX), introduced in the United States in the aftermath of Enron, has important IT governance implications for listed US companies, their foreign subsidiaries, and foreign companies that have US listings. It applies to all Securities and Exchange Commission (SEC)-registered organizations, irrespective of where their trading activities are geographically based. SOX is fundamentally different from the Combined Code, and from codes of corporate governance adopted elsewhere in the OECD, in that compliance is mandatory, rather than 'comply or explain'. This aspect, combined with significant potential sanctions for individual directors, drives SOX compliance requirements through the supply chain to organizations not directly subject to its requirements.

While the Act lays down detailed requirements for the governance of organizations, the three highest-profile and most critical sections – which were implemented in phases – are 302, 404 and 409 (see Table 2.1).

The SEC, which is responsible for implementation of SOX, has relevant information available at https://www.sec.gov/info/smallbus/404guide/intro.shtml (archived at https://perma.cc/5BSZ-58VQ), and the Sarbanes–Oxley website itself is at https://sarbanes-oxley-101.com (archived at https://perma.cc/2AFS-GUYA).

Internal controls and audit

Under SOX, managers are required to certify the company's financial reports, and both managers and an independent accountant are required to certify the organization's internal controls. In almost every organization, financial reporting depends on the IT infrastructure, whether it is for the rendering of an invoice, the effective operation of an ERP system, or an integrated, organization-wide management information and control system. Unless appropriate internal controls are built into this infrastructure, managers will not be able to make the required certification.

The SEC mandated US companies to use a recognized internal control framework that has been established by an organization that developed the framework through a due process, including the inviting of public comment. One widely used framework is known as the COSO framework or, to give it its own title, the 'Internal Control – Integrated Framework', which contains the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (www.coso.org (archived at

TABLE 2.1

	Section		
	302	404	409
Requirement	Quarterly certification of financial reports	Management's annual certification of internal controls	Monitor operational risks
	Disclosure of all known control deficiences	Independent accountant must attest report	Material event reporting
	Disclosure of acts of fraud	Quarterly reviews of updates/changes	'Real-time' implications – four business days allowed for report to be filed
Responsibility	CEO	Management	Management
	CFO	Independent accountant/auditor	Independent accountant/auditor

https://perma.cc/BD5A-K68N)). The sponsoring organizations included the AICPA, the Institute of Internal Auditors, the Institute of Management Accountants and the American Accounting Association. The PCAOB (Public Company Accounting Oversight Board, at www.pcaobus.org (archived at https://perma.cc/T6VV-SAM7), created under SOX to oversee the activity of the auditors of public companies in the United States) expects the majority of public companies to adopt the COSO framework, and its Auditing Standard No. 5 (AS No. 5), dealing with audit of internal control over financial reporting, assumes that the COSO framework (or one substantially like it) will have been adopted.

COSO identifies two broad groups of IT systems control activities: general controls and application controls. General controls are those controls that ensure that the financial information from a company's application systems can be relied upon. General controls exist most commonly as part of an information security management system (such as that identified in ISO/IEC 27001). Application controls are embedded in the software to detect or prevent unauthorized transactions. Such controls can be used to ensure the completeness, accuracy, validity and authorization of transactions.

AS No. 5 goes on, at paragraph 36, to require that 'the auditor also should understand how IT affects the company's flow of transactions. The auditor should apply paragraph 29 and Appendix B of Auditing Standard No. 12, *Identifying and assessing risks of material misstatement,* which discuss the effect of information technology on internal control over financial reporting and the risks to assess.'

IT controls are fundamental to financial control, and ISO/IEC 27001 sets out a structured approach to identify risk and select appropriate mitigation for that risk.

Enterprise risk management

Enterprise risk management (ERM) has emerged over the last few years as a fundamentally new way for organizations to approach risk. This is driven partly by the extensive overlap between the risk management requirements of SOX, Basel 2/3, and corporate governance regimes elsewhere in the world, as well as ongoing changes in the global information economy. Organizations face new and complex risks in a rapidly changing business, technological and regulatory environment. They cannot afford not to identify and control against all areas of risk – including those that might remain unidentified or unforeseen, such as currency fluctuations, human resource issues in foreign countries, changing or disappearing distribution channels, corporate governance and regulatory pressures, and the range of risks associated with technology, information and intellectual assets.

An ERM process should ensure that a uniform approach to risk identification, measurement and treatment is taken across the organization. ISO31000 is emerging as a widely recognized standard for enterprise risk management.

COSO ERM framework

COSO's internal control framework has become the *de facto* standard for companies complying with SOX. COSO started work on developing a separate risk management framework in 2001. This framework, the 'Enterprise risk management – integrated framework', was designed to provide a common framework, 'key principles and concepts, a common language, and clear direction and guidance' (as stated in its executive summary, COSO, 2004). This framework expands on the internal control

framework, providing a broader and more robust focus on ERM; because it incorporates the internal control framework, organizations could (as COSO suggests) move towards implementing an ERM framework to satisfy their internal control needs as well as their broader business risk management needs.

COSO defines ERM as 'a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives'. It is a definition broad enough to encompass the Basel 2 definition of operational risk as well as that in SOX. It is about achieving the organization's business strategy and it deals with strategic, operational, reporting and compliance goals or objectives.

The COSO ERM framework has eight components:

- internal environment;
- objective setting;
- event identification;
- risk assessment;
- risk response;
- control activities;
- information and communication;
- monitoring.

An effective ERM framework will be one in which all eight components are present and functioning effectively in each of the four categories of objectives. Of course, the components will not function identically in every organization, and implementations will be less formal and structured in smaller organizations than in larger ones. The COSO ERM framework comes with detailed implementation guidance and any organization considering adoption of such a framework should acquire and study both the ERM framework and the 'Application techniques'. There are a number of general points that relate to IT governance.

ERM involves analysis and treatment of all business risks – those that are transferable or insurable as well as a wide array of traditionally non-insurable risks – the ERM implementation process is an inherently collaborative one that requires teamwork among many disciplines within

an organization. Depending on the business sector it will require, for instance, risk management, credit management, treasury and accounting input, as well as operational management, marketing, R&D and the law department. It is better to have someone specifically charged with leading the ERM process, and this person should have the full support of the CEO, the board and the managers.

Regulatory compliance

Organizations have traditionally responded to regulatory compliance requirements on a law-by-law, or department-by-department basis. That was, last century, a perfectly adequate response. There were relatively few laws, compliance requirements were generally firmly established and well understood, and the jurisdictions within which businesses operated were well defined.

Since the turn of the century, all that has changed. Rapid globalization, increasingly pervasive information technology, the evolving business risk and threat environment, and today's governance expectations have, between them, created a fast-growing and complex body of laws and regulations – such as the DPA 2018, PECR and Computer Misuse Act in the United Kingdom, and HIPAA, SOX and GLBA in the United States – that all have an impact on the organization's IT systems. While global companies are in the forefront of finding effective compliance solutions, every organization, however small, and in whatever industry, is faced with the same broad range of regulatory requirements.

These regulatory requirements focus on the confidentiality, integrity and availability of electronically held information, and primarily – but not exclusively – on personal data. Many of the new laws – such as US state data breach laws and the EU GDPR – appear to overlap and, although there is a growing body of case law on the subject, there is still little established legal guidance as to what constitutes compliance but also new laws and regulatory requirements continue to emerge. Increasingly, these laws (such as California's SB 1386 and the CCPA) have a geographic reach that extends to organizations based and operating outside the apparent jurisdiction of the legislative or regulatory body. Similarly, US organizations can find themselves subject to the requirements of foreign regulations, such as the GDPR, the EU-US Safe Harbor regulations or Canada's PIPEDA. In the US public sector, FISMA sets out very clear information security requirements for all

government bodies in the United States, while the HMG Security Policy Framework sets out UK requirements.

In the face of new, blended, complex, evolving, advanced and persistent threats to their data, organizations have business and regulatory obligations to protect, maintain and make that data available when it is required. They have to do this in an uncertain compliance environment where the rewards for success don't grab headlines, but the penalties for failure do. Fines, reputation and brand damage and, in some circumstances, jail sentences for directors are outcomes that every business wants to avoid, and wants to avoid as systematically and cost-effectively as possible.

In most instances, there is not yet a comprehensive body of tested case law and proven compliance methodologies to which organizations can turn in order to calibrate their efforts. There are no technology products which, of themselves, can render an organization compliant with any of the data security regulations, because all data security controls consist of a combination of technology, procedure and human behaviour. In other words, installing a firewall will not protect an organization if there are no procedures for correctly configuring and maintaining it, or if users are habitually able to bypass it (through, for instance, Instant Messenger, internet browsing or the deployment of rogue wireless access points).

The adoption of an externally validated, best-practice approach for information security – one that provides a single, coherent framework that enables simultaneous compliance with multiple regulatory requirements – is, therefore, a solution to which organizations are increasingly turning.

While the relevant statutes and compliance requirements are covered in more detail in Chapter 26, the key planning issue at this point is the idea that the ISMS be designed in such a way that it helps the organization meet its regulatory and contractual compliance requirements. ISO27001 is emerging as the single international standard that provides a consistent, widely-recognized international standard for information security management and assurance.

IT governance

Listed companies, in both the United Kingdom and the United States, are expected to take proactive steps to identify and meet their compliance requirements. Continued pressure from governments, institutional shareholders and the general public will ensure that directors have little 'wiggle

room'; non-compliance is likely to have a terminal impact on the careers of those directors who think that it is a viable option. The guidance, both from the FRC and as laid out in the PCAOB's Auditing Standard No 5 (which replaced AS No 2 in 2007), points inexorably at the need for organizations to create and implement IT governance frameworks.

There is an IT governance portal at www.itgovernance.co.uk (archived at https://perma.cc/AR35-5XF4). It reflects clearly the principles that have been set out above, as well as the broader belief that organizations should integrate their IT strategies and their business strategies, because it is mission-critical for most organizations to share information efficiently with customers, partners, suppliers and a wide range of stakeholders. As organizations recognize that IT management should have a fundamental input to the development of business objectives and business strategies, so information technology is increasingly being seen as a critical enabler of business processes. At the same time, many of the management issues around information technology are changing from concerns about financial controls and other threats and vulnerabilities that also need to be controlled to responding to the challenges and opportunities made possible by information technology.

The most practical and effective way for directors to handle their IT governance obligations and, specifically, their information security risks, and to be seen to do so systematically and comprehensively, is to adopt and implement an information security policy and ISMS capable of being independently certified (also described as 'registered') as complying with ISO27001. The standard provides the only independently developed public framework for the management of information security. While compliance with the standard does not of itself confer immunity from legal obligations, it does point clearly to management's implementation of best practice in regard to effective IT governance, and can therefore help to develop competitive advantage in an organization and be available as part of a potential legal defence against any of the threats identified above.

ISO27001 itself says that an ISMS 'preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.' This, in a nutshell, is why organizations are adopting ISO27001 in growing numbers.

3

ISO27001

Benefits of certification

There are a number of direct, practical reasons for implementing an information security policy and information security management system (ISMS) that is capable of being independently certified (or registered) as compliant with ISO/IEC 27001. An accredited certificate tells existing and potential customers that the organization has defined and put in place effective information security processes, thus helping create a trusting relationship. A certification process also helps the organization focus on continuously improving its information security processes. Of course, above all, certification, and the regular external review on which ongoing certification depends, ensures that the organization keeps its information security system up to scratch, and therefore that it continues to ensure its ability to operate.

Most information systems are not designed from the outset to be secure. Technical security measures are limited in their ability to protect an information system. Management systems and procedural controls are essential components of any really secure information system and, to be effective, need careful planning and attention to detail.

ISO27001 provides the specification for an ISMS, and in the related code of practice, ISO/IEC 27002, it draws on the knowledge of a group of experienced information security practitioners in a wide range of significant organizations across more than 50 countries to set out best practice in information security controls. An ISO27001-compliant system will provide a systematic approach to identifying and combating the entire range of potential risks to the organization's information assets, the variety and impact of which were described in Chapter 1. It will also provide directors of UK- and US-listed companies, directors of UK government organizations covered by the government's 'Orange Book', and directors in the supply chains of both

public- and private-sector organizations with both a systematic way of meeting their responsibilities under the UK Corporate Governance Code, the FRC Risk Guidance and Sarbanes–Oxley, as described in Chapter 2, and the wide range of interlocking data protection and privacy legislation to which they are subject, and demonstrable evidence that they have done so to a consistent standard.

It also enables organizations outside the United Kingdom and United States to demonstrate that they are complying with their national corporate governance requirements as well as the data protection and privacy legislation in their local jurisdiction. Equally importantly, an ISO27001 certificate enables an organization to demonstrate to any of its customers that its systems are secure; and this, in the modern, global information economy, is at least as important as demonstrating compliance with local legislation. ISBS 2010 identified that 68 per cent of large UK organizations had been asked by their customers to demonstrate compliance with information security requirements. Possession of a suitably scoped ISO27001 certificate enables a supplier cost-effectively to answer the information security and governance questions in request for proposal (RFP) and pre-tender questionnaires.

Certification to ISO27001 of the organization's ISMS is a valuable step. It makes a clear statement to customers, suppliers, partners and authorities that the organization has a secure information management system. Many countries in the world have their own central accreditation body (in the United Kingdom, it is the United Kingdom Accreditation Service: UKAS). This central accreditation body accredits the competence of certification bodies – who might be based inside or outside the country – to perform services in the areas of product and management system approval.

Organizations should use only accredited certification bodies when seeking ISO27001 certification. This makes sure that the certification process is independent, is of an appropriate quality, using competent personnel (including auditors), and ensures that any certificate awarded will be recognized internationally. A certificate is usually valid for up to three years.

The history of ISO27001 and ISO27002

BS7799, the UK standard that preceded ISO27001, was originally the outcome of a joint initiative by the then Department of Trade and Industry in the United Kingdom and leading UK private-sector businesses. The working

party produced the first version of BS7799 in February 1995. This was originally simply a code of practice for IT security management. Organizations that developed ISMSs that complied with this code of practice were able to have them independently inspected but there was initially no UKAS accredited certification scheme in place, and therefore formal certification was not possible. An alternative solution, known as 'c:cure', was adopted to provide a framework for recognizing implementation of the standard, and was available from April 1997. The confusion around c:cure and the absence of UKAS-accredited certification resulted in uptake of certification to the standard being much slower than anticipated, and c:cure was effectively withdrawn as an option late in 2000.

BS7799 underwent a significant review in 1998. Feedback was collated and in April 1999 a revised standard was launched. The original code of practice was significantly revised and retained as Part 1 of BS7799, and a new Part 2 was added. Part 1 was retitled 'Code of Practice for Information Security Management' and provided guidance on best practice in information security management. As a code of practice, BS7799 Part 1 took the form of guidance and recommendations. Its foreword clearly stated that it was not to be treated as a specification. It became internationalized as ISO/IEC 17799 in December 2000.

BS7799 Part 2, titled 'Specification for Information Security Management Systems', formed the standard against which an organization's security management system was to be assessed and certified. BS7799 Part 2 underwent a further review during 2002, and a number of significant changes were made. This version remained current until it was first internationalized as ISO27001 in 2005

BS7799–2 was internationalized as ISO/IEC 27001:2005 in 2005, and ISO17799 was revised at the same time, thus ensuring that the correspondence between the controls in the two standards would be maintained. ISO17799 was, without further amendment, bought into the new ISO/IEC numbering sequence for information security management standards in 2007 and identified as ISO/IEC 27002:2005, with the change in nomenclature being described in the document as a corrigendum!

ISO27001 and ISO27002 underwent extensive revision from 2008 onwards, and new, updated versions were published in October 2013. These are the current versions, and this book focuses specifically on them.

ISO27001 'forms the basis for an assessment of the Information Security Management System (ISMS) of the whole, or part, of an organization. It may be used as the basis for a formal certification scheme'. It is, in other

words, the specific document against which an ISMS will be assessed. It is the most important standard in the emerging ISO27000 family; it provides a specification, against which an ISMS may be assessed. Apart from ISO/IEC 27000, which is nominatively referenced from ISO27001, the other standards provide useful guidance and advice, and have no mandatory effect.

The ISO/IEC 27000 series of standards

ISO27001 is part of a much larger family, of which ISO/IEC 27000 is the root for a whole numbered series of international standards for the management of information security. Developed by a joint committee of the International Organization for Standardization (ISO) in Geneva and the International Electrotechnical Commission, these standards now provide a globally recognized framework for good information security management.

The correct designations for most of these standards include the ISO/IEC prefix, and all of them should include a suffix, which is their date of publication. Most of these standards, however, tend to be spoken of in shorthand. ISO/IEC 27001:2013, for instance, is often referred to simply as ISO27001.

Many of the standards have been previously published and are undergoing periodic revision; others are still under development. This book deals specifically with ISO27001 and ISO27002, but it will refer, where appropriate, to guidance contained in the supporting standards listed here. Organizations interested in using or applying these standards should acquire copies, which are available through www.itgovernance.co.uk/standards (archived at https://perma.cc/LHC2-ZRB5) in both hard copy and downloadable formats:

- ISO/IEC 27000 – ISMS Overview and Vocabulary;
- ISO/IEC 27001 – ISMS Requirements;
- ISO/IEC 27002 – Code of Practice for Information Security Controls;
- ISO/IEC 27003 – ISMS Guidance;
- ISO/IEC 27004 – Information Security Management – Monitoring, Measurement, Analysis and Evaluation;
- ISO/IEC 27005 – Information Security Risk Management;
- ISO/IEC 27007 – Information Security Management System Auditing;
- ISO/IEC TR 27008 – Guidelines for Auditors on Information Security Controls.

There are then standards that provide guidance on specific topics such as the integrated implementation of ISO 27001 and ISO 20000-1 (the service management system management standard), information security governance (ISO 27014) and organizational economics (ISO TR 27016).

The following are standards detailing requirements for certification bodies seeking accreditation for their ISMS certification scheme:

- ISO/IEC 17021-1 – Conformity Assessment: Requirements for bodies providing audit and certification of management systems – Part 1: Requirements;
- ISO/IEC 27006 – Requirements for bodies providing audit and certification of Information Security Management Systems.

Finally there are standards that provide sector-specific guidelines on the implementation of an ISMS. They include: inter-sector and inter-organizational communications (ISO 27010); telecommunications (ISO 27011); cloud services (ISO 27017); processors of personally identifiable information in public clouds (ISO 27018); energy utility (ISO 27019); and the health sector (ISO 27799).

A full list of current and emerging ISO27000 standards is maintained at www.itgovernance.co.uk/iso27000-family (archived at https://perma.cc/X9EL-UMEX) and you should ensure that the version you are using has been updated to reflect the 2013 standard.

Use of the standard

As a general rule, organizations implementing ISO27001 will do well to pay close attention to the wording of that specific standard itself, and to be aware of any revisions to it. Nonconformity with revisions or corrigendums will jeopardize an existing certification. ISO/IEC 27001 itself is what any ISMS will be assessed against; where there is any conflict between advice provided in this, in a supporting standard or any other guide to implementation of ISO27001 and ISO27001 itself, it is the wording in ISO27001 that should be heeded.

An external auditor will be assessing the ISMS against the published standard, not against the advice provided by this book or any third party. It is critical, therefore, that those responsible for the ISMS should be able to refer explicitly to the clauses and intent of ISO27001 and should on that basis be able to defend any implementation steps they have taken.

An appropriate first step is therefore to obtain and read ISO/IEC 27001 itself. Note that ISO27001 uses the word 'shall' to indicate a requirement, whereas the other standards in the family use 'should' to indicate good practice which is not a requirement.

The UK Accredited Certification Scheme was launched in April 1998, and there is an ISMS users' group that enables users to exchange information on best practice and enables members to provide feedback on a regular basis to national standards bodies, and through them to the International Organization for Standardization.

ISO/IEC 27002

In 1998, when the original BS7799 was revised for the first time, prior to becoming BS7799 Part 1, references to UK legislation were removed and the text was made more general. It was also made consistent with OECD guidelines on privacy, information security and cryptography. Its best-practice controls were made capable of implementation in a variety of legal and cultural environments.

In other words, the ISO/IEC 27002 Code of Practice is intended to provide a framework for international best practice in information security controls and systems interoperability. It also provides guidance, to which an external auditor will look, on how to implement controls within a certifiable ISMS. It does *not,* as the standard is currently written, provide the basis for an international certification scheme. The guidance that this book provides in implementing an ISMS will therefore start with the requirements of ISO27001, will then look to ISO27002 for guidance as to the range of actions that could be considered in implementing selected controls, and will look to other best practice sources for more detailed input where relevant.

It is particularly important to note that, while ISO27002 provides international best practice in information security controls, it is not necessarily up to date for more recent changes in the information security environment. It has been written, and rewritten, over a number of years. The speed with which information technology has evolved, and goes on evolving, already means that some of the specific guidance in ISO27002 may be inadequate to deal with newly identified threats and vulnerabilities and the most current responses to them. That does not invalidate ISO27002; it simply creates an opportunity for the practitioner to go beyond IS27002 when necessary.

This book has a bias towards implementing an ISMS within the United Kingdom, as this is where the authors' direct experience was gained. It does also draw on our combined experience, over a number of years, working with organizations around the world on their information security management strategies. Its lessons are directly applicable for all ISMSs that are to be certified by an accredited certification body anywhere in the world.

This book sets out how to implement an ISMS that is capable of certification to ISO/IEC 27001:2013. It will do so broadly within the context of the Microsoft suite of products, as these are the products most widely used in those parts of the world likely to be interested in certification. The implementation steps set out in this book, however, apply in all software and hardware environments. The standard itself was specifically written to be technology independent.

This book will refer very explicitly to ISO27001 and to ISO27002 in order to comment on the implementation steps necessary to reflect the recommendations of ISO27002 and to comply with the standard. However, the reader must obtain current copies of both documents (as well as any others that may appear to be necessary) and use them alongside this book in order to optimize an information security project and gain the full value of this book.

Continual improvement, Plan–Do–Check–Act, and process approach

The 2002 version of the standard for the first time promoted the adoption of a 'process approach' for the design and deployment of an ISMS. This approach, widely known as the 'Plan–Do–Check–Act' (PDCA) model, is familiar to quality and business managers everywhere. While ISO27001:2005 mandated the adoption of PDCA, it is no longer specifically required; what is a specific requirement is the adoption of a suitable and appropriate continual improvement process. For many organizations, this will continue to be the PDCA model but the way is open for organizations that, for instance, already use ITIL or COBIT to adopt instead the continual improvement models from those frameworks. The vast majority of organizations are likely to adopt PDCA, not least because it is an easily understood model which also lends itself to application in integrated management systems which cover (for example) quality, environment, IT service management and

business continuity. This book will assume that the PDCA model is used, and you should therefore make sure that you thoroughly understand it.

The 2013 version of the standard has been designed for better alignment, or integration, with related management systems (eg ISO9000) within the organization. Other ISO standards are being brought into accordance with a consistent high-level structure and common terminology (known as Annex SL, because it is an annex to an ISO directive on standardization) which will simplify management system integration significantly; the concept of a single, integrated management system, embedded within the standard operating processes of the organization, and capable of certification to multiple standards, is becoming much easier for the average organization to achieve.

A note on numbering

ISO27001 adopts the same standard numbering methodology for its clauses and sub-clauses as will other management system specifications. This means that the requirements of the standard (what you have to do if you are to claim compliance with it) are set out in clauses 4–10, with clauses 1–3 being introductory and the annexes being excluded from the requirements.

ISO27002 follows a different numbering sequence, with clauses 1–4 providing general guidance on the use of the standard, and clauses 5 through 18 providing guidance on individual controls. Annex A to ISO27001 is numbered from A5 to A18, in order to match the control clauses in ISO27002. In this book, we refer to Annex A controls by means of the 'A' prefix (as in A.5.1.1.) and to those same controls in ISO27002 by means of the ISO27002 numbering (as in 5.1.1). Where we identify clauses in ISO27001, we are specifically referring to the stated requirements of the standard.

Returning to ISO 27001, the numbering is solely for the purpose of referencing. The standard itself recognizes that the order and number of clauses does not indicate relative importance or an order of implementation.

Structured approach to implementation

Although ISO27001:2013 allows the organization to tackle its clauses in any appropriate order, it makes sense to have a structured approach to the establishment of an ISMS. There are six steps to this 'Plan' stage of a project (using the Plan-Do-Check-Act approach that used to be, but is no longer, prescribed in ISO 27001):

1. Create the management framework: set up your implementation project, define the internal and external context of the organization, identify the requirements of any interested parties and, considering these issues, define the scope of the ISMS; select a continual improvement model and determine your approach to documentation.
2. Obtain top management commitment to the ISMS, define an information security policy, and allocate roles and responsibilities – including a 'management representative'.
3. Define a systematic approach to information security risk assessment and the risk acceptance criteria.
4. Carry out a risk assessment to identify, within the context of the policy and ISMS scope, the important information assets of the organization and the risks to them. This is where you assess the risks.
5. Identify and evaluate options for the treatment of these risks, selecting, where required, the control objectives and controls to be implemented.
6. Prepare a statement of applicability and a risk treatment plan.

Once these steps have been carried out, you would begin implementation (the 'Do' stage) of the system.

The implementation process will go through its own five steps:

1. Finalize the risk treatment plan and its documentation, including planned processes and any required supporting documentation.
2. Implement the risk treatment plan and planned controls.
3. Arrange appropriate training for affected staff, as well as awareness programmes.
4. Manage operations and resources in line with the ISMS.
5. Implement procedures that enable prompt detection of, and response to, security incidents.

The 'Check' stage – which drives continual improvement activity – has, essentially, only one step: monitoring, reviewing, testing and audit. However, monitoring, reviewing, testing and audit is an ongoing process that has to cover the whole system, and a certification body will want to see evidence of an effective internal audit programme in relation to the ISMS as part of its certification activities.

Testing and audit outcomes should be reviewed by managers, as should the ISMS in the light of the changing risk environment, technology or other

circumstances; improvements to the ISMS should be identified, documented (where necessary) and implemented. This is known as the 'Act' stage. Thereafter, it will be subject to ongoing review, further testing and continuous improvement.

A 'mini-PDCA' approach could also be applied to each control or group of controls, with the 'Check' phase contributing to the 'measures of effectiveness' that will eventually feed into the management review (see Chapter 4).

This book takes a sequential approach to the establishment and implementation of an ISMS. In reality, once they realize the scale of the information risks they face, many organizations will want to tackle a number of the necessary tasks in parallel. Certainly, as many organizations will come to ISO27001 with some information security structures already in place, an alternative approach built around completing an initial 'gap analysis' which compares the requirements of ISO27001 with the ISMS processes already in place and then builds the ISMS project as, in effect, an information security improvement plan designed to close those gaps, may also be a practical approach. In taking such an approach, however, bear in mind that an effective management system is one in which the way arrangements to address the requirements of the standard relate to and work with one another in order to provide a repeatable and dependable system that delivers required outcomes is more important than simply addressing individual clauses.

If component tasks of establishing the ISMS are being carried out in parallel, or the organization already has elements of an ISMS in place and is driving gap analysis-based improvements toward the objective of ISO27001 conformance, it will be critically important to first have a thorough understanding of all the requirements of ISO27001 as well as a strong project management methodology to keep everything together.

Implementation issues

Implementation of an ISMS will have significant impacts on the way people work. It should be seen as a business project, not an IT or information security project. Effective leadership, top management support, change management and internal communication are all essential components of any successful ISO27001 system roll-out. An overview of key issues that will contribute to a successful implementation is set out below with more specific information and analysis in later chapters.

Clause 6.1 of the Standard requires the organization to consider any issues identified as part of its assessment of internal and external context, as well as the requirements of interested parties (both of which are discussed further in Chapter 5), and assess how these might impact the project to establish an ISMS and the bearing they may have on the longer term effectiveness of the ISMS. This requirement should be addressed as part of creating the project and management framework; the authors recommend that the implementation project itself produces and maintains a project-level risk log. While one of the highest-potential impacts might be assigned to the risk associated with gaps in senior managers' understanding *and* commitment, there may be other project-level risks arising from the organizational context: a currently lax security culture, for instance, creates different implementation challenges than one that is already tightly and centrally controlled.

Management system integration

Some organizations that tackle ISO27001 already have an ISO9001 certificated quality management system in place, and may also have certifications to ISO14001, OHSAS 18001 and other standards, such as ISO20000 and ISO22301. ISO encourages integration of quality and other management systems. The ISMS should be integrated with the quality management and any other management system to the greatest extent possible (not forgetting that any management system needs to be integrated with the business if it is to deliver on all the benefits that it can offer). The adoption of a (largely) consistent high-level structure, common core text and terms and definitions across new and revised ISO management system standards since October 2013 lends itself to a single management system that addresses requirements from multiple standards. In other words, the way in which an organization addresses context, top management commitment, internal audit, continual improvement and documentation can be largely the same for each and every management system standard it adopts.

In the case, therefore, where an organization already has a management system based on this consistent approach (commonly referred to as Annex SL after its then position in the ISO Directives for standardization – just after Annex SK and before Annex SM), implementation of ISO27001 is simply going to be the *extension of* an existing management system to include information security management, not bringing in a whole new

management system. This is an important message that should, in this circumstance, underpin the change management and communication plans; the smaller the perceived mountain, the more quickly will an organization set out to climb it.

In circumstances where the organization does not already have an existing ISO9001-certified management system and wishes for guidance on the documentation, document control (authorization, version control, status, etc aspects of producing management system documents) and records issues of ISO27001, it should obtain and use the guidance in any current manual on the implementation of ISO9001:2015. Note that the ISO27001 specifications for document control (clause 7.5) include the control of records.

The organizations that are accredited to offer certification to ISO27001 are usually listed on the websites of national accreditation bodies. Not all of them offer a truly integrated certification service. Each organization's website will set out what it does, and the links on the site should be followed to explore the offerings of each company.

Documentation

As set out above, the organization should adopt, for its ISO27001 system, at least the same documentation principles as are required for ISO9001. A properly managed ISMS will require documentation. Clause 7.5 of the standard describes the minimum documentation that should be included in the ISMS to meet the requirement that the organization maintain sufficient records to demonstrate compliance with the requirements of the standard. The types of documents that are typically required for an effective ISMS include the following:

- The information security policy, the scope of the ISMS (including the internal and external issues, and the requirements of interested parties), the risk assessment methodology and risk assessment results, the control objectives, the statement of applicability (developed as described in Chapters 5 and 6). These might, together with a description of the Continual Improvement (PDCA) approach, and the rules for document and record control, form the core of an ISMS manual.
- Evidence of the actions undertaken by the organization and its management to specify the scope of the ISMS (business architecture diagrams. organization charts, network maps, etc) the minutes of board and steering committee meetings, as well as any specialist reports).

- A description of the management framework (steering committee, etc). This could usefully be related to the organizational structure chart.
- The risk treatment plan and the underpinning, documented procedures (which should include responsibilities and required actions) that implement the specified controls. A procedure describes who has to do what, under what conditions, or by when, and how. A work instruction is an even more detailed description of how to perform a specific task. Procedures (there might be one for each of the implemented controls) and work instructions might be identified in the ISMS documentation, but would be subject to a lower level of authorization than the manual.
- The procedures (which should include responsibilities and required actions) that govern the management and review of the ISMS. These should be developed in line with the guidance contained in this chapter.

The ISMS documentation should be controlled documents, available to all staff. It can be done in paper form but is most effective either on a shared drive, an intranet, a SharePoint server or through a document management and policy support software tool. SharePoint is increasingly widely used and it ensures that the current version of any procedure is immediately available to all members of staff without inconvenience. Remember that any shared resource will have its own challenges in terms of organization and control; ownership of assets, archiving and data integrity are key issues. SharePoint installations should be subject to their own specific governance arrangements if they are to produce maximum benefits.

A structured numbering system should be adopted that ensures ease of navigation of any manual or related documentation and ensures that initial document issue is controlled, that replacement pages and changes are tracked and that the manual is complete. Staff should obviously be trained in how to use the ISMS; this is usually best done as part of the staff induction process.

Clearly, there will be a number of security system documents that themselves need to be subject to security measures. These will include documents such as the risk assessment, the risk treatment plan and any non-public versions of the statement of applicability, which contain important insights into how security is managed and which should therefore be classified and restricted in accordance with the type of information classification system described in Chapter 9. Access should be limited to people with specified ISMS roles, such as the information security adviser.

ISO27001 clearly recognizes that there is no such thing as a 'one size fits all' approach. Instead, it recommends that the ISMS documentation be scaled to reflect the complexity of the organization and its security requirements.

The ISO27001 ISMS Documentation Toolkit (www.itgovernancepublishing.co.uk/product/iso27001-2013-isms-standalone-documentation-toolkit (archived at https://perma.cc/JGK5-DPVY)) was created specifically to accompany this book. It contains a comprehensive set of ISMS documents that are designed for adaptation to meet the specific requirements of any individual organization.

Leadership

Leadership, like all key business initiatives, has to be provided from the top. The whole of clause 5 of the standard deals with leadership and sets out a number of ways in which top management must evidence their commitment to information security in the organization.

This is very much a clause that looks for 'Tone from the Top'. Ideally, the CEO should be the driving force behind the programme, and its achievement should be a clearly stated goal of the current business plan. The CEO needs to understand completely the strategic issues around IT governance and information security and the value to the company of successful certification. The CEO has to be able to articulate them and to deal with objections and issues arising. Above all, he or she has to be sufficiently in command of this part of the business development to be able to keep the overall plan on track against its strategic goals. The chairperson and board should give as much attention to monitoring progress against the ISO27001 implementation plan as they do to monitoring all the other key business goals. If the CEO, chairperson and board are not behind this project, there is little point in proceeding; certification will not happen without clear evidence of such a commitment. This principle, of leadership from the top, is of course essential to all major change projects.

No certification body will certify an ISMS without getting firm evidence of the commitment of senior managers. If this commitment is not clearly demonstrated, the ISMS simply will not be adequate and the risks to the organization will not have been properly recognized or fully addressed, and the strategic business goals are unlikely to have been considered.

Change management

There have been many books written about change management programmes and initiatives. Many such programmes fail to deliver the benefits that have been used to justify the expense of commencing and seeing them through. Successful implementation of an ISMS does not require a detailed change management programme, particularly not one devised and driven by consultants. What it does require is complete clarity among senior managers, those charged with driving the project forward and those whose work practices will be affected as to why the change is necessary, about what the end result must look like and why this result is essential.

The design and implementation of the ISMS should be driven by a project team that is drawn from those parts of the organization most likely to be affected by its implementation as well as a very small number of functional experts, including HR or personnel experts. The balance is important: a properly functioning ISMS depends on everyone in the business understanding its processes and applying its controls, and if the project team is made up of a preponderance of non-technical people, it is more likely to produce something that everyone in the business understands. The team certainly should include at least one experienced project manager, who will be responsible for tracking and reporting progress against the planned objectives. The project team or sponsor should report directly to the CEO (or equivalent management authority that has responsibility for the entire scope of the ISMS) and have the appropriate delegated authority to implement the board-approved plan. Clause 5.1.c requires the provision of adequate resources to establish the ISMS, and this is the first step to doing so.

There needs to be an outline timetable and top-level identification of responsibilities and the critical path to completion. This should be prepared by the project team and, once it has been critically tested by the CEO and top managers, approved by the board. This plan should fit onto two sides of A4 and should provide sufficient scope for those who will have to implement it to find appropriate solutions to the many operational challenges that there will be.

A key preliminary step in any successful change programme is to identify and isolate, or convert, potential opposition. Where an ISMS roll-out is concerned, there is sometimes internal resistance from the IT department. There are a number of possible reasons for this, including the desire of the head of IT not to lose control of IT security, the IT department's desire to maintain its mystique and the fear that its existing controls might be found

to be inadequate. This is not surprising. ISO27001 does require the organization's board and senior management to take control of its ISMS and the whole organization to get behind and understand key aspects of security policy. The resistance of the IT department must be expected and overcome at the outset. There are circumstances where this can lead to a change in IT staff, either forced or unforced, and the organization should expect this and prepare appropriate contingency plans.

Training will be an important facilitator of the change programme. ISO27001 requires that those who have key roles within the ISMS are appropriately competent (clause 7.2) and this might cover ISMS implementation (for the person/people determined as having responsibility for ensuring the ISMS meets the requirements of ISO 27001, as per clause 5.3 a) and audit competence, as well as initial training for the project team in the principles of ISO27001, the methodology of change and project management and the principles of internal communication. Staff throughout the business will need specific training in those aspects of security policy that will affect their day-to-day work. The IT manager and IT staff will all need competency in information security, and if this needs to be enhanced by training, this should be delivered by an organization that recognizes and understands the technical aspects of ISO27001 training.

Communication

Underlying any successful change management programme, and especially necessary for the successful roll-out of an ISMS, is a well-designed and effectively implemented internal communications plan. Compliance with clause 7.4 (which deals with communication) suggests that key components of this plan might include the following:

- Top-down communication of the vision – why the ISMS is necessary, what the legal responsibilities are, what the business will look like when the programme is complete and what benefits it will bring to everyone in the organization.
- Regular cascade briefings to all staff on progress against implementation objectives. These briefings should quickly become part of the existing organizational briefing cycle, so that ISO27001 progress becomes part of the normal business process – 'just another thing that we're doing'.
- A mechanism for ensuring that key constituencies and individuals within the business are consulted and involved in the development of key

components of the system. This ensures that they buy in to the outcome and to its implementation.

- A mechanism for ensuring regular and immediate feedback from people in the organization or in affected third-party organizations so that their direct experience of the initial system as it is implemented is used in the evolution of the final version.
- These face-to-face communications should be underpinned with an effective information sharing system. Most usually, this will be part of the corporate intranet, on which regular progress reports as well as detailed information on specific aspects of the ISMS are posted. E-mail alerts can tell staff to access the intranet for new information whenever it is posted and the site could encourage feedback by means of a 'write to the CEO' function. Organizational Facebook and Twitter accounts could also be pressed into service as part of the project.

Reviews

Clause 9.1 of the standard requires the effectiveness and performance of the management system, as well as effectiveness of relevant controls to be measured and monitored and for management to carry out periodic reviews of the effectiveness of the ISMS. This will be discussed in some detail in Chapter 6. The records of the management body (to be discussed in Chapter 4) that is responsible for implementing the ISMS should document that these reviews were carried out on particular dates, what the results of the reviews were and what actions, if any, were required as a result.

Continual improvement and metrics

Clause 10.2 of the standard requires the organization 'to continually improve the suitability, adequacy and effectiveness' of the ISMS. The corrective action requirements of clause 10.1 are met by an effective ISMS audit programme (Chapter 27), competent review and management of nonconformities (which often, for the ISMS, involves the information security manager), the incident response procedures (Chapter 24) and related documentation. Prevention, as a specific process, has been removed from the standard, as the ISMS itself is now seen as the preventive tool that management deploys in order to prevent compromises of information security.

The combination of effective monitoring, measuring, and corrective action processes, together with a formal review process and strong internal audit structure, within the context of an ISMS developed in line with the recommendations of this book, will enable an organization to start demonstrating its approach to continual improvement. A long-term approach to continual improvement must include measuring the effectiveness of the ISMS and of the processes and controls that have been adopted. ISO27001 requires effectiveness measurements (also see Chapter 6 and ISO/IEC 27004) to be undertaken and results from them included in the input to the management review meeting. Clearly, information security as an organizational function needs to be measured against performance targets in just the same way as are other parts of the organization. In order to develop a useful set of metrics, an organization will have to identify what to measure, how to measure it and when to measure it.

Some of the areas that should be considered for measurement include the effectiveness and value adding capability of the incident handling process, the effectiveness and cost savings provided by staff training, the improvement in efficiency generated by access controls and external contracts, and the extent to which the current scope is meaningful and relevant in the changing business environment.

4

Organizing information security

It is both practical and sensible to consider the organization's information security management structure at an early stage in the implementation process. This does, in fact, need to be thought through at the same time as the information security policy is being drawn up, as set out in Chapter 5. An effective information security management structure also enables the risk assessment (to be discussed in Chapter 6) to be carried out effectively.

The second control category in Annex A to the standard, in clause A.6.1, is 'Internal organization'. Controls are selected to meet business, regulatory or contractual requirements (the baseline security criteria), or in response to the risk analysis (see Chapter 6); there is a business requirement to put an information security management structure in place from the start of the ISO27001 project. The control objective of control A.6.1 is to 'establish a management framework to initiate and control the implementation and operation of information security within the organization'.

This objective encourages the creation of the management information security forum identified in earlier versions of the standard. More importantly, it no longer prescribes any specific management structure; the key requirement is management's active support for and commitment throughout the organization to the ISMS project. Without this, neither certification nor the project itself will be successful. Clause A.6.1.1 of ISO27002, says that information security responsibilities should be defined and allocated (which reflects also the requirement of ISO27001 clause 5.3) and explains, what best practice expects in terms of the allocation of roles and responsibilities. At the same time, the competence requirements of Clause 7.2 should also be considered.

Internal organization

ISO27002 echoes the requirement that managers should actively support security within the organization through 'clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities'. In practical terms, this means that managers should set up a top-level forum or steering group to ensure that there is clear direction and visible management support for security initiatives within the organization. It could be part of an existing management body, which might be appropriate in a smaller organization where the members of the top management team will also, broadly, be the members of an information security forum. More usually, it will be a separate cross-functional body, adequately resourced for its responsibility, reporting to a member of the top management team and reflecting top management support and commitment. In this book, we will usually refer to this management group as 'the forum'. The effectiveness of this forum will be fundamental to both the effectiveness of the ISMS and compliance with clauses 5.1, 5.2 and 5.3 of the standard.

ISO27003, the formal guidance on ISMS implementation, identifies roles for an information security committee and an information security planning team. The information security committee should have delegated management responsibility for information security within the organization. The information security planning team is responsible for planning implementation of the ISMS, resolving inter-departmental conflict and ensuring that the ISMS project runs to plan. In practical terms, in most organizations, the forum which was described earlier will usually evolve into an information security committee which effectively has governance responsibility for information security. In most organizations, it makes sense for the forum to have both roles: ownership of the ISMS and responsibility for planning and deploying it. In much larger organizations, it is usually sensible to follow the guidance of ISO27003: senior managers, who might be involved in the forum or committee, are not usually able to take part in the actual project work. Towards the end of the project, it is usually practical to merge the two groups, retaining an appropriate mix of roles and skills on the information security committee or future forum so that the ISMS can be maintained and developed after certification.

An effective approach to establishing the forum would be to seek membership from all levels of the organization, and from all parts of the organization that are likely to be affected by the ISMS project. Including, for instance,

those who handle incoming physical mail, IT helpdesk staff, and user representatives will help the forum fully consider all relevant practical issues before making policy or procedure recommendations.

Once the ISMS has been fully established, the forum could become the information security committee identified by ISO27003, or could simply continue to be the forum. Whatever, it should meet at least twice a year and preferably quarterly. All its activities should be formally documented, together with its decisions and the reasons for them. Copies of all material presented at the meetings should be retained, and subsequent meetings should track actions agreed, report on progress for each of them and document these steps. This group should be responsible for:

1. Identifying information security goals and strategy that meet the organization's requirements; ensuring that goals are communicated and understood, checking whether there are adequate resources for achieving them, and whether the ISMS is properly integrated into the organization's processes and business as usual.
2. The review and approval of the organization's information security policy, which must be explicitly agreed and supported by top management setting the scope of the ISMS, ensuring that information security objectives and plans are established, identifying internal and external issues and the requirements of interested parties, and agreeing how roles and responsibilities should be allocated. This should include appointing, or agreeing the appointment of, the manager responsible for information security within the organization, together with the key responsibilities of the role; this role could be given the explicit responsibilities identified in clause 5.3: to ensure that the ISMS conforms to the requirement of ISO27001 and to report to Top Management on the performance of the ISMS.
3. Ensuring that sufficient resources are provided to develop, implement, operate and maintain the ISMS.
4. Monitoring changes in exposure of key organizational information assets to major threats, deciding (within the context of any existing organizational risk treatment framework) acceptable levels of risk and ensuring that awareness of these threats is developed, as well as ensuring that the importance of complying with the ISMS is adequately communicated to the organization.
5. Ensuring that procedures and controls are implemented that are capable of promptly detecting and responding to incidents, as well as the review

and oversight of information security incidents. Receiving reports from the information security manager on the status and progress of specific implementations, security threats, results of reviews, audits, etc and ensuring that adequate steps are taken to implement findings or deal with non-conformities.

6 The approval of major initiatives (such as any individual initiative associated with the implementation of ISO27001) to improve information security within the organization, including security aspects of systems acquisition.

7 Establishing means of monitoring and ensuring compliance with the policy and reviewing the effectiveness of these measures periodically.

8 Ensuring that information security objectives and requirements meet the business objectives.

9 Ensuring that control implementation is coordinated and effective across the organization.

10 Ensuring that adequate steps are taken, on an ongoing basis, to continually improve the ISMS.

Management review

ISO27001 introduces, at clause 9.3, a requirement for a management review of the ISMS, and this should take place at predetermined intervals agreed by the board, whenever there have been significant changes to the organization's risk environment, or business organization, and at least annually. The review process is similar to that required by ISO9001, and ISO27001 sets out clearly and in adequate detail the minimum inputs and outputs expected of such a review, which, ideally, should be carried out by the forum and, again, involve top management. The inputs are all discussed at appropriate points in this book, and the information security manager should be made responsible for gathering together the inputs and communicating, to all concerned, the outputs (decisions) of the review.

Management reviews should be fully documented, with an agenda, with minutes, and with follow-up actions. In integrated management systems, management review is likely to consider all aspects of its integrated management system: quality, environment, IT service management, information security and so on.

The information security manager

Although good practice expects one manager to be made responsible for the co-ordination of all security-related activities, this is not a specific requirement of ISO27001. There are potential conflicts between accepted good practice, the requirement for impartiality in ISO27001 clause 9.2.e, control A.6.1.2 for segregation of duties, and the resources actually available to the organization. One should pay particular attention to the standard, to the competences required of the role, and to reality when finalizing these arrangements. It is also worth bearing in mind that the organization may – depending on the expertise of the person selected for the information security manager role – also need access to specialist information security advice; if this is not provided by the person who manages the ISMS, it could be provided by someone else. That is entirely a matter for the organization concerned.

Practical experience demonstrates that one person really will need to be charged with managing the ISMS project, and this person should be appropriately qualified. He or she could be appointed before the forum is set up, and his or her brief could include the formation of the forum. The benefit in this route is one of speed and, potentially, of simplicity. The board member who has been charged with responsibility for ensuring implementation of the ISMS could simply select and appoint an appropriate person and an initial project team, who could then take things forward. The selection and training of the members of a forum are potentially more time-consuming, and the period during which they are learning their roles will precede the point at which they are competent to select and appoint an appropriate information security manager. The organization may not wish to pursue this slower route.

While the information security manager does not need to be the same person as is appointed as the organization's information security expert (the skill sets required for the managerial role, particularly in a larger organization, are likely to be different from those required for the security expert's role), this person will still need adequate training in information security matters, and the discussion later in the chapter, headed 'Specialist information security advice', should be read in conjunction with this section. Obviously, the person selected for the managerial role will need to be an effective manager with well-developed communications and project management skills.

This manager should be charged with a number of defined and key activities. Depending on the culture and structure of the organization, these could include:

1. Establishing the management information security forum (unless the organization chooses to establish the forum first and then ask the forum to select the manager).
2. Formalizing, with the forum, a standard glossary of terms. Words like 'risk', 'threat' and 'incident' mean different things to different people and it makes practical sense to have a standard corporate glossary that provides standard definitions of all the terms that are used for information security or in any of the management systems. ISO/IEC 27000 is a good place to start, in that it contains a full set of terms applicable to the ISMS. Other terms from other standards and frameworks (eg business continuity, or ITIL, or COBIT) could be added as required.
3. Developing, with the forum, the security policy, its objectives and strategy.
4. Defining, with the forum, the scope of the ISMS, taking into account internal and external issues and the requirements of interested parties.
5. Briefing the forum on current threats, vulnerabilities and steps taken to counter them.
6. Working with risk owners to carry out the initial information security risk assessment.
7. Ensuring risk owners identify changed risks and that appropriate action is taken.
8. Ensuring that the risk is managed by agreeing with the board, risk owners and the forum, the organization's approach to risk management, the risk treatment plan and the level of assurance that will be necessary.
9. Selecting control objectives and controls that, when implemented, will meet the objectives.
10. Preparing the statement of applicability and risk treatment plan.
11. Recording and handling security incidents, including establishing their causes and determining appropriate corrective and/or preventive action.
12. Reporting to the forum on progress with implementing the ISMS, and on incidents, issues, security matters and current threats.
13. Ensuring management reviews are carried out as required.

14 Monitoring compliance with the standard and reporting to management on the effectiveness of the ISMS.

15 Driving continual improvement activity across the entire ISMS.

The cross-functional management forum

The concept of a cross-functional forum has disappeared from ISO27001. It was a sensible idea and organizations should consider setting one up. The driving logic is that information security activities would be coordinated by representatives from different parts of the organization with relevant roles and job functions. This is particularly relevant for larger organizations, where security activity needs to be coordinated across a number of divisions, companies or sites, each of which may have its own information security manager or adviser. This cross-functional forum could, in smaller organizations, be integrated into the management information security forum discussed earlier. The range of activities that might be carried out by this cross-functional forum are:

1 agreeing, across the organization, specific roles and responsibilities in respect of information security;

2 agreeing the specific methodologies and processes that are to be used in implementation of the information security policy;

3 agreeing and supporting cross-organizational information security initiatives;

4 ensuring that the corporate planning process includes information security considerations;

5 assessing the adequacy and coordinating the implementation of specific controls for new systems, products or services;

6 reviewing information security incidents;

7 supporting the communications strategy and ensuring that the whole organization is aware of the way in which information security is tackled.

There is a lot of overlap between the possible functions of the management forum and the cross-functional group described earlier in this chapter. An external certification auditor will want to know how the two key functions – coherent management of information security and coordination of information security-related activity – have been tackled. One route, clearly, is

for each forum to have very clearly differentiated functions and for the reporting lines between the two to be drawn very unambiguously.

Usefully, in all but the largest organizations these two forums can be combined. Practically, this is sensible, as otherwise the structural issues of relating the two forums and of clarifying what issues are dealt with at which level can create unnecessary bureaucracy. Where two separate groups are set up, the first to operate more at the strategic level and the second more at the implementation level, the time of the information security and functional specialists will be stretched as they will need to contribute to both. The managerial benefits of combining the two groups are so significant that this book will proceed on the basis that this is the appropriate route, and our use of the term 'forum' from now onwards will refer to this combined group.

The detailed work of the management forum is then best dealt with by asking the manager responsible for information security to draw up, outside the formal meetings, proposals as to how each of the issues should be dealt with.

These proposals should then be tabled, discussed and agreed by the forum. All meetings of this forum should be documented, as should actions agreed and progress against them.

The ISO27001 project group

Ideally, the forum should be set up at the outset of the project and be chaired by the senior executive or board member who is designated as responsible for the implementation of the ISMS. The forum should, initially, and in most smaller organizations, also be the project team that sees implementation through to successful conclusion and whose ongoing role clearly evolves from this initial responsibility. This intention should be clearly documented in the project plan and in the first minutes of the forum and/or terms of reference for the group.

Members

Members of the forum, a number of whom need to be in senior positions within the organization, should be selected from across the organization. Key functions that should be represented are quality or process management, human resources, training, IT and facilities management; these may all have to change their working practices significantly as a result of the

decision to implement an ISMS. Apart from the manager responsible for information security and the trained information security expert, the most critical representation will be from HR, sales, operations and administration. These tend to be the functions in which the majority of the organization's personnel are employed and the ones that will be most affected by the implementation of an ISMS. While the people invited to represent these functions should be among the most senior and widely respected individuals within them, it can also be beneficial to draw in representation from more junior ranks and certainly from end users. Without this perspective, the forum may be inadequately aware of issues 'on the ground', and may arrive at conclusions that, in practical terms, are difficult to implement.

As discussed earlier, the change process that ISO27001 implementation will require has a cultural impact. It is critical that those most able to represent and articulate the needs and concerns of the key parts of the organization are included on the working party. Without their involvement, there is unlikely to be the 'buy in' necessary for the ISMS to be effectively developed and implemented.

Clause 7.2 of the standard requires the organization to ensure that all personnel are competent to perform the tasks assigned to them in the ISMS. This will require the organization to determine the competences required, first of the forum members and later of those charged with implementation. This chapter has pointed at the range of competences that may be required, and final decisions should be documented. See also the discussion on training in Chapter 8.

As soon as the members of the implementation team have been chosen, and once their mission and role have been explained to them, it will be necessary to give them some initial exposure to the standard and to information security. There are a number of ways that this can be done. One is to send them on a Foundations of Information Security Management training course, which is a one-day seminar designed to inform and assist delegates who need a clear introduction to the principles and objectives of information security management. Such a course should be suitable as a general introduction to the subject for people who will not need to become too deeply involved in many of the details of the ISMS. Another, obviously, is to give them each a copy of this book; the first six chapters are probably the ones that will be most useful for the 'lay' members of the implementation team.

It is equally critical that all members of the working party understand clearly that their role is to put together and implement an ISMS that meets

the board's requirement. The CEO needs to set this requirement clearly in front of the working party. There will undoubtedly be divergences of opinion between members of the team at many points during the implementation process and on a wide variety of issues. This should make for a stronger ISMS, as what emerges will be more likely to meet all the requirements of the organization. However, if the process is not managed effectively, this working party could also be the graveyard of the information security strategy.

When healthy disagreement degenerates to competition and open warfare, there will be little or no progress; if what emerges from the process is simply the view of one faction or another, it will not be successfully implemented.

Equally, it is possible for the working party to become bogged down in procedural issues or to be ultra-cautious in how it tackles the implementation challenge. While the danger of the project dragging on can be dealt with by setting a very clear date by when implementation must be complete (even to the point of writing it into the individual performance objectives of all the members of the team), it can still fail because the working party simply does not work effectively. Clearly, therefore, the most important choice to be made in respect of both the implementation working party and the management forum into which it will evolve is that of its chairperson.

Chairperson

The choice of chairperson of this group is usually critical to its success, both as a group and in terms of how the rest of the organization views and responds to it. The chairperson needs, therefore, to be someone who is capable of commanding the respect of all members of the working party. He or she needs to be wholly committed to achieving the goal of a certified ISMS within the board-agreed timetable. He or she needs to be pragmatic and prepared to 'think outside the box' in identifying solutions to organizational problems that are affecting implementation. This person should not be from any one of the organization's support functions, as this will usually brand the project as an unimportant one. The project should on no account be led by an IT person, as the implementation of an ISMS simply cannot afford to be seen as only an IT project. The chairperson should, preferably, have a broad managerial responsibility within the organization as well as experience in implementing cross-organizational change projects. Ideally, he or she will be the CEO or the main board director who has been charged with implementation of the board's security policy. In smaller organizations, this

person might also be the manager responsible for information security; in larger organizations, where this is likely to be a full-time role, the manager responsible for information security should properly report to the chairperson of the forum. The need for segregation of duties needs also to be considered.

Not only is the structure outlined here the most effective method for delivery of the ISMS, but it is also very clear evidence of commitment from the very top of the organization to its implementation. The external ISO27001 auditor should be suitably impressed.

Records

Meetings should be scheduled ahead of time, to ensure that everyone who will be needed can record them in their diaries and be present. The frequency of meetings during the implementation phase will reflect the urgency and complexity of the implementation plan. In practical terms, meetings held fortnightly for the first few months of the implementation timetable can contribute to building momentum in it. After that, they can drop to monthly events. Once implementation is complete, the forum might meet on a quarterly basis or when there are significant changes or business issues to consider. The forum should decide how often it needs to meet, set out its reasons and record the decision.

Meetings do not, of course, require physical attendance. They can take place by videoconference or by teleconference. What matters is that all members are able to take part, that they have adequate notice of the meeting and that the meetings are properly managed and documented.

Normal meeting principles should be established and maintained. All meetings should have an agenda and an attendance record, and action points and key decisions should be recorded in the minutes, with information about who is responsible for what actions and within what timescales. The minutes should be retained as part of the quality records, and the external auditor is likely to want to review them. In practical terms, the quality function or PMO within the organization is usually best placed to provide the secretariat to this group.

While the external auditor will be particularly interested in what has been done about action points identified in the minutes, forum meetings can easily degenerate into long reviews of the minutes and actions arising from the previous meeting. Pragmatically, if the minutes are scheduled on the agenda to be dealt with at the end of the meeting, right before ‘any other

business', meetings will be quicker and the organization will make substantially faster progress with the overall implementation. The chairperson should, prior to the meeting, have ensured that action points have been dealt with; this enables them to be reported on very quickly when the appropriate point on the agenda is reached.

As a matter of principle, one of the authors insists on starting meetings at the scheduled time, irrespective of how many people are in the room, and refuses to sum up progress so far for late arrivals. In the long (and sometimes the short) run, everyone learns to arrive on time.

Allocation of information security responsibilities

ISO27001, at control A.6.1.1, says that 'all information security responsibilities shall be clearly defined'. While the information security policy may provide general guidance as to who is responsible for which information security risk, this guidance is likely to be very broad, particularly if the policy model suggested in this book is adopted. It will not necessarily be clear to individual employees, from the policy statement, what their specific responsibilities will be. In any case, the organization will need to define clearly who is responsible for which risks, which security process and/or information asset and may have to look at geographic or site responsibilities as well.

For instance, while the need for an information security manager is clear, it is nevertheless sensible to identify individual owners of information security assets throughout the organization and confirm to them in detail and in writing their responsibilities in respect of these assets. This is an incredibly effective way of ensuring that the security of individual information assets is properly maintained on a day-to-day basis. Clause 8.1.2 (Ownership of Assets) of ISO27002 provides more information on this issue but does not add significantly to what we have said here.

There are generic responsibilities for members of particular groups of staff. The responsibilities of the members of the forum have been discussed, as have those of the information security manager. Those mentioned below could provide the basis for defining individual responsibilities within the organization and should be drawn more specifically to reflect the organizational structure and systems.

IT departments should be accountable for the overall security of the system(s) for which they are responsible. This includes threat identification, assessing risks, managing projects, reviews and reporting on activity. Server room security should be another of their responsibilities.

Local system administrators will have specific responsibilities for user registration and deletion, system monitoring, preparing security procedures, managing change control with defined boundaries and handling data back-up, designing application security, implementing internal controls and testing contingency and fall-back plans.

System managers should be responsible, at the system level, for threat identification, assessing risks, implementing selected security controls, securely configuring the system(s), setting up the user ID and password system, setting up system security monitoring, implementing change control and setting up all necessary security procedures and maintaining and testing business continuity plans.

Network managers should be responsible (at the individual domain or independent network level) for network perimeter threat identification, assessing risks, implementing selected network security controls (including firewalls), securely (designing and) configuring the network, setting up security monitoring, implementing change control, setting up security procedures and maintaining and testing network recovery plans.

Site managers should be responsible, in respect of the physical site for which they are the nominated manager, for threat identification, assessing risks, implementing selected physical controls (including perimeter controls), fire detection and response, utility services and their back-up, delivery and dispatch controls, and maintaining and testing the site's business continuity plan. For the purposes of the ISMS, every site from which the organization operates should have at least one site manager. Where the site is a large and complex one, perhaps including a number of organizations or divisions of organizations, then a number of site managers may be required. A method of coordinating their activity will then be necessary. Clearly, the site manager's responsibilities would normally be combined with a number of other line management responsibilities.

IT users throughout the organization should be required to be aware of and follow the organization's security policy and procedures, maintain the clear desk policy and other physical security procedures, follow the password and access control procedures, back up data (which is particularly important for notebook and mobile users) and comply with requirements in respect of social media and report security incidents.

Third parties should be required to comply with their contractual responsibilities. They should also be aware of the host organization's security procedures and practices.

The identification of these individual responsibilities will be done throughout the process of pulling together the detailed information security

procedures; it is important for the forum members and the information security manager to be aware from the outset that this will be a key component of the drafting process for every procedure. It would be as well to adopt, at the outset, a standard template for the drafting of processes or procedures that includes headings such as 'scope', 'purpose', 'process or procedure owner', 'individuals or roles identified as having responsibilities under this document', 'date for review (if any)'. These are in addition to the parameters required to effect suitable document control and confidentiality or availability status. There may be other items worth adding to such a template; the purpose is to ensure that all the key components are systematically included in each new document.

Specialist information security advice

ISO27001:2013 does not have a specific requirement for an organization to deploy a specialist information security adviser. The reality, however, is that specialist advice may, at least, be necessary.

The organization may need advice from in-house or specialist external security advisers. While ISO27002 no longer provides detailed guidance on this issue, our view is that, while not all organizations will wish to employ their own specialist internal adviser and may prefer that a non-specialist internal adviser is given the security management responsibility, this person should have access to external advice (perhaps through a mentoring scheme or other support contract) that provides specialist input covering any areas in which the in-house person is deficient. It is particularly important that, in the areas of security technology and information technology generally, specialist advice is retained and is easily available. Technology, vulnerabilities, threats and defences are evolving so fast that it is difficult for any single individual to keep completely on top of them all.

While there is a discussion in Chapter 8 of this book about information security education and training, particularly for the users of information security facilities, it is at this point appropriate to look at the qualifications that might be appropriate for an in-house specialist adviser or that one might expect to be evidenced by an external specialist.

Bear in mind, while considering this issue, the requirement at clause 7.2 of the standard, that the organization must determine its requirements in terms of the competence necessary to perform tasks associated with information security, ensure that it is has those competences available, and that it keeps records to prove it.

One option is for the organization to employ someone to provide the required specialist information and security advice who appears to be qualified by experience. However, it can be difficult for an inexperienced recruiter to identify someone who is really adequately experienced for this role. As correct selection of this person is critical to the early success of the ISO27001 project, it is worth taking a structured approach to resolving the issue.

It is recommended that any organization pursuing ISO27001 specifies from the outset that its information security adviser be appropriately qualified and that if someone who does not have a formal qualification but claims to be qualified through experience is recruited for the role, he or she be required (as a condition of continuing in employment beyond the initial probationary period) to demonstrate this competence by acquiring an appropriate qualification.

It is now possible to obtain a postgraduate qualification in information security management from the UK's Open University. This course, numbered M886, is designed to help employees understand, create and manage both strategic and operational aspects of information security and it uses this book as its core textbook. We believe that this course is unique.

The International Board for IT Governance Qualifications (www.ibitgq.org (archived at https://perma.cc/XS5A-53RW)) has developed a range of ISO27001-focused certified training courses. These include a certified Lead Implementer and a certified Lead Auditor course. IBITGQ-accredited training organizations are authorized to deliver training courses that prepare individuals for the externally set and monitored examination that leads to these certifications. Those who have attended these courses will all have a good understanding of key ISO27001 issues:

- information security management concepts (confidentiality, integrity, availability, vulnerability, threats, risks and countermeasures, etc);
- current legislation and regulations that have an impact on information security management in the United Kingdom (or in the jurisdiction in which the course is delivered, as appropriate);
- current national and international standards, frameworks and organizations that facilitate the management of information security;
- the current business and technical environments in which information security management takes place – security products, malicious software (malware), relevant technology, etc;
- the categorization, operation and effectiveness of a variety of safeguards.

The British Computer Society (BCS), based in Swindon (www.bcs.org (archived at https://perma.cc/BQS6-994U)) is another link for any organization pursuing ISO27001. The BCS website describes a range of training programmes and regimes that are applicable to information professionals. More helpfully, it also describes the Information Systems Examination Board (ISEB) qualifications. The ISEB Certificate in Information Security Management Principles (CISMP) is designed to provide a foundation of knowledge for individuals who have security responsibility as part of their day-to-day role or who are likely to move into a security or security-related function.

Globally, there are now about 30 different vendor-neutral information security certificates, including those sponsored by ISACA and by the International Information Systems Security Certification Consortium (ISC 2). There is further discussion of training in Chapter 8.

The organization should, in appointing its information security adviser, pay as much attention to the quality of the individual as to his or her qualifications and formal experience. The nature of information security threats is always changing, and the technology and context within which an organization is maintaining its information are in constant flux. The information security adviser needs to be able to respond to new threats and find and protect vulnerabilities in new technologies that the organization wants to deploy to improve its competitive advantage. This requires a flexibility of thought allied to a depth of experience and a structured, balanced – and open-minded – approach to all the information security issues that the organization will encounter. Of course, high-quality people need appropriate compensation packages; this will be money well spent.

Segregation of duties

Another issue that has to be considered when setting up the ISMS is what the approach to segregation of duties should be. Control A.6.1.2 of ISO27002 provides for duty segregation, with the explicit objective of reducing the likelihood of misuse of organizational facilities or misappropriation of organizational assets. The concept of segregation of duties is unlikely to be new to most readers of this book and the sensible approach is to extend the segregation rationale currently deployed within your internal control framework to cover your ICT activities as well. Key areas for consideration should include segregation between those who request user access

rights and those who configure them; between those who do audits and those who are to be audited; those who update ISMS documentation and those who approve them for release; those who configure security controls (such as firewalls or IDS) and those test them – and between those who develop software and those who test or deploy it.

It should be noted that, although segregation of duties is available for selection as a control, it is not a specific requirement of the standard; the only requirement of the standard in this regard is in clause 9.2, which deals only with the requirement for internal audits to be impartial. The statement in the general introduction to the standard, that the ISMS should be scaled to the size of the organization is also relevant: smaller organizations will be much less able to segregate duties than larger ones.

Contact with special interest groups

As a practical matter, even where the organization recruits or appoints and trains a specialist security adviser, it is imperative that this person has access to specialist advice that covers the entire spectrum of information security.

It is equally imperative that there is a method of remaining current with changing issues in the information security environment. The environment and the threats within it change so rapidly that an organization systematically has to keep on top of them. Your national CERT (Computer Emergency Response Team) or WARP (Warning, Advice and Reporting Point) are good starting points. The most important site for a Microsoft network is, of course, www.microsoft.com (archived at https://perma.cc/GX4A-BB7A). This carries a host of critical and relevant information, as well as updates and downloads, and should be consulted on a regular basis. The two most critical parts of the Microsoft site, from a security perspective, are the Safety & Security Centre (www.microsoft.com/en-gb/security (archived at https://perma.cc/YY9A-6W65)) and Microsoft technet (https://technet.microsoft.com/en-gb (archived at https://perma.cc/PN7T-F4KH)). Every information security adviser should ensure that Microsoft best practice is integrated (where appropriate) into the organization's ISMS.

There are a number of sources of regular information on information security issues. One is the information services available from this book's website; it has a governance bias and is designed to be complementary to this book and to the range of information and support services provided by IT Governance Ltd. Other specific information security magazines worth

investigating are: *SC Magazine* – available online and offline, with editions for the United Kingdom, the United States and Asia Pacific, with a website at www.scmagazine.com (archived at https://perma.cc/BQS6-994U); and *Infosecurity Today Magazine* – website: www.infosecurity-magazine.com (archived at https://perma.cc/ZP6A-4BWB). We believe their subscription cost offers clear value for money.

There are also online services and information security websites. One online service worth exploring is https://searchsecurity.techtarget.com (archived at https://perma.cc/5SP8-ECWB), which provides a wide range of relevant, up-to-date information security advice.

Another critical website for the information security adviser is the site of the Computer Security Resource Center (US National Institute of Standards and Technology): https://csrc.nist.gov (archived at https://perma.cc/Z5WL-42XB). This site is an excellent information centre resource for information security professionals; in particular, it carries substantial quantities of technical and security information on most issues that will be of interest in setting up a certifiable ISMS.

Attendance at industry exhibitions, such as RSA and Infosec, should also be a standard part of the role. The major annual UK exhibition is Infosec, and details of exhibitions can be obtained through www.infosecurityeurope.com (archived at https://perma.cc/38HY-438C). These shows have a wide range of current products available for review, as well as a series of seminars and addresses on current and upcoming security issues.

Each of these sources of information should supplement regular visits to the Microsoft website as well as those of providers of any other chosen and installed corporate software, including particularly the providers of the chosen firewall and antivirus software. These sites will usually be the first places that identify specific threats to their software and propose solutions. The information security specialist should follow all these information sources on a regular basis and act immediately a new threat or vulnerability is identified. Sometimes the newspapers can identify threats as fast as any other organization; no source of information should be ignored!

There are two straightforward ways of identifying what local or national networks of specialists there might be. The first is by joining the local chapters of relevant professional organizations such as ISACA or ISC2. The second is through the ISO27001 auditor assigned to the organization by the company chosen to provide third-party certification of the ISMS against the standard. Asking the auditor for referrals and contacts is a completely sensible thing to do; the auditor ought to be extremely well linked, and if he or

she is not, then the expertise and current awareness of the auditor, and therefore his or her competence to do an adequate auditing job for the organization, ought to be questioned.

Contact with authorities

ISO27001 says, at control A.6.1.3, that 'appropriate contacts' should be maintained with 'relevant authorities' (law enforcement bodies, fire departments, supervisory or regulatory bodies, ISPs and telecommunications operators) and with 'special interest groups and other specialist security forums and professional associations (eg sources of specialist advice)'. Neither the standard nor ISO27002 sets out what would constitute 'appropriate contacts'; the latter does, however, set out clearly the purpose in maintaining contacts with authorities, which is to enable the organization to take appropriate action quickly, or to obtain appropriate advice, should events (security incidents) require it.

To an extent, this will be considered further in Chapter 26, which deals with business continuity management. For the purposes of this chapter, though, the organization's information security adviser (who should be consulted and involved in all information security incidents) should systematically develop, over the first months in the role, a series of contacts with the local police and, through them, with specialist digital forensics consultants, penetration testers, and the nearest police specialist 'cybercrime' unit (if one exists). The information security adviser should also develop contacts with the organization's contracted providers of information and telecommunications services, and, in particular, with those members of their staff who are responsible for dealing with information security issues, and with local or national networks of information security specialists.

Information security in project management

Control 6.1.5 deals, as the title suggests, with information security in project management. This control can apply to all projects, not just IT or information security projects, from a minor IT implementation through to a major business change project. Information security should be part of 'business as usual' and, therefore, information security risks and objectives should be considered at the outset of each project; where appropriate, a risk

assessment is conducted and specific controls selected and implemented to ensure the organization's information security objectives are not compromised during, or as a consequence of, the project.

Independent review of information security

Control 18.2.1 says the organization should have its implementation of its information security policy independently reviewed. ISO27002 makes it clear that this can include bringing in outside auditors to review the ISMS or bringing in independent third-party certification auditors to certify it; the accredited certification audit meets this control requirement of the standard.

It does, however, recognize (as does any quality management system) that an organization ought to have its implementation of any key system or process reviewed by someone other than the person responsible for implementing it. This is a standard principle of an ISO9001-certificated management system, and any company that has such a management system in place can simply graft an extra responsibility on to those who have the existing ones.

An internal audit function that only has experience in financial audit will not, however, be adequately trained to carry out a quality management system audit. Equally, an audit function that already deals with internal audit of another management system will not be automatically capable of competently conducting an ISO27001 audit.

There is an IBITGQ Internal Audit qualification, and most third-party certification bodies are likely to provide training courses for internal audit teams. Quality system auditing is a necessary basis for ISMS auditing, but is not sufficient. At the very least, the internal auditor should attend a Foundations of Information Security Management course described earlier in this chapter – a one-day seminar for delegates who need a clear introduction to the principles and objectives of information security management. Specific ISO27001 internal auditor courses are available, which are designed to ensure that those internal staff who are taking on an ISMS audit role will have the skills and knowledge they need. Ideally, the organization will have access to an appropriately qualified ISO27001 ISMS Lead Auditor, who can plan and oversee the entire internal audit process, and have an internal audit team that can be deployed to conduct the audits. The IBITGQ (identified earlier in this chapter) has both lead auditor and internal auditor qualifications. Further information on relevant training courses can be accessed

through https://www.itgovernance.co.uk/iso27001-information-security-training (archived at https://perma.cc/L7HP-GBH4).

Summary

The organization should put in place, from the outset, the management framework required by the standard and make it responsible for implementation of the board's information security policy. Initial training of the key people, particularly the specialist information security adviser, is important and worth investing time and money in before starting the process of implementation. Once the groundwork is laid, progress can be quick.

5

Information security policy and scope

Once the information security management structure has been thought through, the initial ISMS establishment issues have been completely understood and the initial training of the key personnel who will be involved in the development of the policy has been put in place, the first and second steps in the Plan phase can be carried through.

Context of the organization

The Standard requires (at 4.1 and 4.2, respectively) that the context of the organization, as well as the requirements of interested parties, be identified (and preferably documented) as a preliminary step to determining both the scope of the ISMS and its overarching policy. This requirement simply forces the organization to consider, from the outset, all those factors which will determine the scope and focus of the ISMS.

ISO27000 defines 'external context' as being, in effect, any of the external factors that the organization has to take into account in creating its business plan and determining information security objectives; these can include sectoral characteristics; business, economic, technological, competitive and other, wider trends (on any geographic level) as well as the perceptions and requirements of stakeholders and regulatory bodies. 'Internal context' includes any of the aspects or characteristics of the organization that should be taken into account in designing the ISMS. These could include business model; governance structure, roles and accountabilities; organizational culture, capabilities and attitudes; existing policies, strategies, architectures and frameworks; and existing contractual relationships. Internal and external

context should be thoroughly documented. In particular, the needs and requirements of interested parties – legal, regulatory and contractual – should all be listed, preferably in a comprehensive database which enables you to describe exactly how those various information security requirements are met within your ISMS. (See also Chapter 26 on compliance.) This step enables you to determine your baseline security criteria: the specific set of security controls that must be implemented in order to meet existing business (eg IPR protection), regulatory (eg DPA) or contractual (eg PCI DSS) requirements.

Information security policy

The information security policy is the founding document of the ISMS. It should set out top management's vision for information security in the light of key strategic business objectives and reflect the key limitations and opportunities that determine the scope of management's ambition for the ISMS. Clause 5.2 of the standard (and control A.5.1) contains the basic requirement. Creation of an information security policy is, however, not always as straightforward as it seems. It may be an iterative process (particularly in complex organizations dealing with complex information security issues and/or multiple domains), and the final form of security policy that is adopted may therefore have to reflect the final risk assessment that has been carried out and the statement of applicability that emerges from that.

Clause 5.2 sets out the requirements for the ISMS policy. The scope of the ISMS, and therefore the policy itself, must take into account the characteristics of the business, its organization, location, assets and technology. The policy must include or reference a framework for setting information security objectives and establish the overall sense of direction. It must take into account all relevant business, legal, regulatory and contractual security requirements. It must establish the strategic context (for both organization and risk management) within which the ISMS will operate. It must establish criteria for the evaluation of risk and the structure of the risk assessment. Of course, top management must approve it.

The security policy will also have to be regularly reviewed and updated in the light of changing circumstances, environment and experience. As a minimum, if there is no earlier reason for the board to review its policy, it should be reviewed annually and the board should agree that the policy remains appropriate (or otherwise) to its needs in the light of any changes to the business context, to the risk assessment criteria or in the identified risks.

Initially, the information security policy is a short statement (we think organizations should aim for it to fit a maximum of two pages of A4) that is designed to set out clearly the strategic aims and objectives that will guide the development of the ISMS. The policy may go through a number of stages of development, particularly in the light of the risk assessment, but the final version must satisfy clause 5.2 of the standard and should appropriately reflect the good practice that is set out in clause 5 of ISO27002. Proof that the policy has been approved by top management, has been published and communicated internally and is reviewed regularly (usually annually, as a minimum), with any changes similarly published and communicated, will enable the organization to satisfy this requirement of the standard.

The key questions for the initial policy statement to succinctly answer are:

- Who?
- Where?
- What?
- Why?

Usually, the manager who has been charged with leading the implementation of the ISMS will be charged with drafting a security policy and board paper that proposes how these questions should be answered. This paper should seek to be as objective as possible in working through the possible answers to these four questions so that the board can identify and focus on those issues that require clarification or where difficult decisions may be necessary.

A copy of that section of the minutes (preferably signed off by the chairperson as a correct copy) of the board meeting in which the security policy was debated and adopted should be filed with the security policy documentation. It can be a controlled record and it does, for audit purposes, provide useful and immediate evidence of the process by which the policy was adopted, and of any amendments to it. This, together with the proposal that was put to the board, is the first part of the evidence that top management have met the requirements of clause 5.1 in terms of committing to the creation of an ISMS whose objectives are compatible with the strategic aims of the organization.

The policy itself should then be issued as a controlled document and made available to all who are doing work within its scope; copies could be posted on all internal noticeboards, both the physical and electronic ones. There are other methods of communication; what matters is that the

communication is effective. These copies of the policy document should of course be clearly marked as controlled copies, to ensure that they are updated to reflect any changes that take place. Copies handed out as part of training or awareness seminars, or to third parties, should be marked as uncontrolled copies.

Who?

'Top management' has to be completely behind and committed to the ISMS; therefore, the policy statement must be issued under their authority and there should be clear evidence, in the form of written minutes, that the policy was debated and agreed both by the board as a whole and by any separate management steering group. Any revisions to the policy should also be debated and agreed by both the board and the steering group.

From a practical point of view, it is worth keeping the policy statement as simple, as comprehensive, as principled and as strategic as possible so as to allow managers adequate freedom to respond to changing business and security circumstances in implementing it without needing to return to the board and the forum for the policy itself to be freshly agreed.

It will also require participation by all employees in the organization and should reflect the needs of customers, suppliers, shareholders and other third parties. This is part of the context of the ISMS referred to earlier. In thinking through the security policy, the board and the forum will need to consider what impact it will have on these constituents and/or audiences and the benefits and disadvantages that the business will experience as a result of this.

Where? (scope of the policy and the ISMS)

Those parts of the organization within which the policy is going to apply need to be clearly identified. The standard is explicit that the scope must be determined once the context of the organization (internal and external issues) and the requirements of interested parties have been established. This may be done on the basis of corporate, divisional or management structure, or on the basis of geographic location. There should be logical access to all assets within scope, and consideration given to occurrences of those assets at other sites. In other words, the dependencies and interfaces of the assets within scope will need to be made clear within the scope statement. In larger, more complex organizations, network maps, organization charts, business architecture diagrams and information flow charts may be useful tools for

clarifying possible scope statements. ISO27003 says that, as part of the scoping exercise, the assets on which the key business processes depend should be identified, their ownership clarified and their security requirements analysed.

A virtual organization, a cloud-based business or a dispersed, multi-site operation, may each have security issues different from those that affect one located on a single site. In practical terms, a security policy that encompasses all of the activities within a specific entity for which a specific board of directors or 'top management' team is responsible is more easily implemented than one that is to be applied to only part of the entity. It is important to ensure that the management team that is implementing the policy does actually have adequate control over the operations contained within scope and that it will be able to give a clear mandate to implement the security policy within that scope. The section in Chapter 6 'Identify the boundaries' should also be read at this point, particularly as the ISMS is required to be considered within the overall organizational context.

It is critical, if there are aspects of the organization's activities or systems that are to be excluded from the requirements of the security policy, that these are clearly identified – and explained – at this stage. Multi-site or virtual organizations will need to consider carefully the different business requirements of their different sites and the security implications of them. There should be clear boundaries ('defined in terms of the characteristics of the organization, its location, assets and technology') within which the security policy and ISMS will apply. Any exclusions should be openly debated by the board and the steering group, and the minutes should set out how and why the decision was taken. It is possible that, in fact, divisions of the organization, components of the information system or specific assets will not be able to be excluded from the scope, either because they are already integral to it, or because their exclusion might compromise a dependent business process or undermine the information security objectives themselves. It must therefore be clear that any exclusions do not in any way compromise key business processes or undermine the security of the organization to be assessed.

This is particularly important where outsourced processes are concerned. Outsourced processes (but not the organizations to which they are outsourced) should be included in the ISMS scope and subject to appropriate controls. This is sensible. You need assurance that your key business processes – even if operated by third parties – are still operated within your risk tolerance.

Auditors will be assessing how the management team applies its policy across the whole of the organization that is defined as being within the scope of the policy and should be expected to test to their limits the boundaries of the stated scope to ensure that all dependencies and interfaces with security-related processes have been identified and adequately dealt with.

In reality, as stated earlier, the process of designing and implementing an effective ISMS may be made simpler by including the entire organization for which the board has responsibility. Even so, there will still need to be decisions about client and supplier access as well as any disaster recovery site. Access to information assets within the scope (for example, data hosted on a server that is within scope) from a geographically remote site will have an effect on the arrangements for maintaining the confidentiality, integrity and/or availability of that data, and so in one way or another will be a concern of the ISMS. These issues all need to be addressed through the scope statement and the risk assessment.

There is an argument, in large, complex organizations, for a phased approach to implementation. Where it really is possible to define adequately a subsidiary part of the organization, such that its information security needs can be independently assessed, it may be possible to gain substantial experience in designing and implementing an ISMS, as well as a track record of success and the momentum that accompanies it, such that a subsequent roll-out to the rest of the organization can be carried through successfully and smoothly. These considerations apply to any large, complex project, and the appropriate answer depends very much on individual organizational circumstances.

It would certainly be a mistake to define the scope too narrowly. While it may appear, on the surface, to be a quick and easy route to certification, it is in fact a route to a worthless certificate. Any external party assessing the organization's ISMS will want to be sure that all the critical functions that may affect its relationship, and the information about which it is concerned, are included, and limiting the scope will compromise this objective.

The overall issue of scoping is certainly one where experienced, professional support can be helpful in assessing the best way forward.

What?

The statement that the top management 'is committed to preserving the confidentiality, integrity and availability of information' is at the heart of a security policy and an ISMS. It is important to define precisely the key terms

used in the policy, and we recommend that the definitions contained in ISO27000 are used. For ISMS purposes, 'information' should be very widely defined:

> Information [can be] printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, [or] spoken in conversation.

In other words, appropriate protection is required for *all* forms of information:

Confidentiality [is defined as] information not made available or disclosed to unauthorized individuals, entities or processes.

Integrity [is defined as] the property of accuracy and completeness.

Availability [is defined as] being accessible and usable upon demand by an authorized entity.

Availability is particularly important to cloud-based businesses, or those engaged in e-commerce or social media. A business that depends for its very existence on the availability of its website, but that fails to take adequate steps to ensure that the site is up, running and running properly at all times, is likely to fail as a business much more quickly than a traditional bricks-and-mortar business that is unable to open its shop doors for a few days.

Members of the board, the management team and the staff of the organization should all understand that these are the definitions of these words, and they should be prominently described and set out in the early briefings to staff and in internal communications. Auditors from certification bodies are likely to check (probably randomly) that staff understand what these words mean, and while they will not look for staff to remember these definitions verbatim, they will want staff to demonstrate practical understanding of how the pursuit of these aspects of information security is likely to have an impact on their own work. This level of understanding is required, as a minimum, so that each member of staff is able to recognize and react appropriately to a security incident. Information security incident management is covered in Chapter 24.

There is also the point at which the organization needs to determine its criteria for accepting risks and to identify the levels of risk it will accept. It is a truism to point out that there is a relationship between the levels of risk and reward in any business. Most businesses, particularly those subject to FRC Risk Guidance and similar standards, will want to be very clear about

which risks they will accept and which they won't, the extent to which they will accept risks and how they wish to control them. The management team needs to specify its approach, in general and in particular, so that the business can be managed within that context.

Risk assessment is discussed further in Chapter 6.

Why?

Information security, broadly speaking, may be defined as: 'the protection of information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities' and is also 'essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image'. The initial staff communication process should set out clearly the nature of the threats faced by the organization and the possible costs, in both financial and non-financial terms, of information security breaches. The information provided in this book can be used for that purpose, but, wherever possible, local and/or industry-specific information should be sought and used, as this gives immediacy and currency to the possible threats. Illustrations of the possible consequences to the organization itself should be developed in order to help all those involved to fully appreciate the need for the ISMS.

The 'where' and the 'what' answers above form the basis of the statement of the scope of the ISMS. There is a further, and more detailed, discussion of some of the issues related to scoping the ISMS in the next chapter, in the context of risk assessments. There should be a single document that identifies the internal and external context as well as the requirements of interested parties and, in that light, sets out clearly the organization(s) that fall within the scope of the policy, which locations, which assets and which technologies. This statement of policy is an essential initial document, which not only helps focus the development of the ISMS but also makes clear to all concerned the seriousness of their responsibilities. It may be sensible, at this stage, to divide the organization into separate security domains. A 'domain' is a discrete logical or physical area of an organization or network that is the subject of security controls designed to protect it from outside access. A domain should be capable of representation on a diagrammatic map. An organization or a network may be made up of one or a number of domains.

A policy statement

The initial policy statement might, therefore, read as follows:

> The board and management of organization Y, which operates in sector Z (or is in the business of Z, etc), located in …, are committed to preserving the confidentiality, integrity and availability of all the information assets throughout their organization in order to maintain its competitive edge, cash-flow, profitability, legal and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with organizational goals, and the ISMS is intended to be an enabling mechanism for information sharing for electronic operations, for e-commerce and for reducing information-related risks to acceptable levels. All employees of the organization are required to comply with this policy and with the ISMS that implements this policy. Certain third parties, as defined in the ISMS, will also be required to comply with it. This policy will be reviewed when necessary and at least annually.
>
> In addition, the policy should cover the following areas:
>
> - It should announce that a top-level management steering group will be established to support the ISMS framework and periodically review the security policy.
> - It should outline the approach to risk management, the criteria against which risk will be evaluated, the structure of the risk assessment and who will be responsible for it.
> - It could briefly identify specific policy requirements, such as access policy, malware stance, mobile working, back-up and roll-over, and security incident reporting.
> - It should contain a commitment to meet other information security or compliance requirements, whether business, regulatory (eg data protection acts), statutory (eg corporate legislation) or contractual (eg PCI DSS).
> - There should be a clear statement of the requirement that information security continue to be aligned to specific business goals and contain a framework for setting information security objectives across the organization.
> - It could explain that all staff will receive security awareness training and specialized staff will receive more specialized training.
> - It could formally state the commitment to comply with, and achieve and maintain accredited certification to, ISO27001.

It must state that the ISMS is subject to continual improvement.

Such a statement would be sufficiently general to cover all the key components of information security for organization Y for the foreseeable future, but sufficiently precise and clear to be effective as a policy statement. It should clearly be approved by the management information security forum and signed by the most senior person in the organization (the chairperson, president, CEO, director-general, etc). A template for an information security policy is included in the ISO27001 ISMS Documentation Toolkit.

The security policy statement can be expanded, in the light of the risk assessment, to take into account the further guidance of clause 5.1 of ISO27002. The policy statement proposed here does, however, meet the requirements of clause 5.2 of ISO27001.

Costs and the monitoring of progress

Any sensible board or management team will, at this stage, also require an estimate of the costs and resources involved in implementing the ISMS, an assessment and quantification of the potential benefits, and an outline implementation plan that describes, at the top level, who will be responsible for doing what and by when. Such a document should be prepared and presented to the board along with the proposed security policy. This document should set out clearly the proposed dates at which the board will be invited to review progress towards final implementation so that it can ensure that its policy is being properly implemented.

As all organizations have their own preferred formats for doing this, this book does not set out how to do it. It only argues that review dates should be realistically spaced and that the plans it approves should allow executive managers sufficient flexibility in implementing a policy that will have to be designed in the light of facts that are not known at the point at which the policy is adopted.

It is suggested that the key points at which progress might be reviewed are:

1 After completion of the risk assessment; the full range of risks to be managed will have been identified.

2 After completion of a draft statement of applicability (SoA). Any costs incurred prior to this should be minimal, but until the SoA defines what

needs to be done, it will not be possible to budget effectively for the implementation.

3 After implementation of the initial suite of procedures that apply the identified controls.

4 After completion of the first cycle of system audits and reviews in accordance with clause 9.2 of the standard and prior to the initial visit by the certification body.

5 Annually, as part of the regular review of the ISMS, to ensure that the budget is being correctly applied and that any new technology issues, threats or vulnerabilities have been taken care of.

It is assumed that the organization will already have well-developed procedures for dealing with projects that are missing key review dates and in which there is overspending or underperformance. The IT Governance website has resources and guidance on effective project governance, and this book will not, therefore, make any proposals about what action should be taken to rectify any shortfalls, but will make the observation that early and vigorous action by the board to ensure that there is compliance with its requirement to design and implement an information security policy and management system will go a long way to proving to the organization the seriousness of the endeavour and thus to bringing about its achievement.

6

The risk assessment and Statement of Applicability

Establishing security requirements

An earlier version of ISO27001 identified three sources for establishing the organization's information security requirements: the risks that the organization faces (business, risks, discussed further below); the risks arising from the compliance and contractual requirements imposed on the organization in each of the jurisdictions in which it operates (compliance requirements in particular are discussed in Chapter 26); and the 'particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations', which are the consequence of the IT architecture the organization has previously established to support its business model.

Risks, impacts and risk management

All organizations face risks of one sort or another on a daily basis. Risk management is a discipline that exists to deal with non-speculative risks – those risks from which only a loss can occur. In other words, speculative risks, those from which either a profit or a loss can occur, are the subject of the organization's business strategy whereas non-speculative risks, which can reduce the value of the assets with which the organization undertakes its speculative activity, are (usually) the subject of a risk management plan (in ISO27001, a 'risk treatment plan'). These are sometimes called permanent and 'pure' risks, in order to differentiate them from the crisis and speculative types.

Risk management plans usually have the following linked objectives, which are:

- to eliminate risks;
- to reduce to 'acceptable' levels the risks that cannot be eliminated;
- to deal with the risks at 'acceptable' levels, in one of the following ways:
  - living with them, exercising carefully the controls that keep them 'acceptable';
  - transferring them, by means of insurance, to some other organization;
  - committing to a plan to reduce the risk to an acceptable level within a defined time frame.

Pure, permanent risks are usually identifiable in economic terms; they have a financially measurable potential impact upon the assets of the organization. The requirements of Sarbanes–Oxley, COSO, the FRC Risk Guidance and, for financial sector organizations, the Basel 2/3 Frameworks have raised risk management – and, in particular, operational risk management – to a core function in most large organizations.

Risk acceptance criteria

Risk management strategies are usually based on an assessment of the economic benefits that the organization can derive from an investment in a particular control; in other words, for every control that the organization might implement, the calculation would be that the cost of implementation would be outweighed, preferably significantly, by the economic benefits that derive from, or economic losses that are avoided as a result of, its implementation. 'Risk appetite' is the phrase used to describe managers' level of preparedness to take risks. The capacity of the organization to absorb loss will be one of the key determinants of risk appetite. The organization uses risk acceptance criteria for determining which risks it will take and which ones it will reject. Alternatively, it could apply controls to reduce risks to a level that it can tolerate.

The organization should define its criteria for accepting risks (for example, it might say that it will accept any risk that has an economic impact less than the cost of controlling it) and for controlling risks (for example, it might say that any risk that has both a high likelihood and a high impact must be controlled to an identified level, or threshold).

Before we turn to a detailed consideration of the risk assessment process, we have to recognize that most organizations will already have made a number of decisions about risks (they have, after all, been in business for a time, dealing with threats and vulnerabilities for real) and will also have implemented a number of controls in order to comply with statutory, regulatory or contractual requirements. The organization will need to decide how it incorporates these existing controls into its ISMS and its risk assessment methodology.

The first, sensible step is simply to recognize, in your risk assessment methodology, that the requirements of interested parties (what we have called the 'Baseline Security Criteria' have led the organization to implement specific controls; identify the interested parties and their requirements as described in Chapter 5 ('Context of the Organization'), and state that the related controls – called Baseline Security Controls – are incorporated as they are into the ISMS. You then have to determine how you handle all the other controls which are already in place, the ones that you adopted at some earlier point to meet specific security criteria at the time. You either review them, now, for adequacy and effectiveness, or you recognize their existence and simply accept them as part of your baseline security control set, focusing your risk assessment on those remaining risks which are not yet appropriately treated. For example, a door is a control but, in assessing the security of a room you recognize that the door is already in place, accept its adequacy as a control, and focus on other entry routes ('attack vectors').

For most organizations, the practical approach is to adopt the baseline security control approach and focus on remaining risks. Thereafter all controls, new and old, can be reviewed for effectiveness as part of the continual improvement programme.

Approach to risk assessment

Approaches to enterprise risk management provide the backdrop against which the requirements of IT governance and ISO27001 should be considered. ISO27001 requires a risk assessment to be undertaken. This is at the heart of the ISMS. Clause 6.1.2 of the standard requires the organization to 'define and apply an information security risk assessment process', which should be appropriate for the organization, its information security objectives and the identified business, legal and regulatory requirements (the baseline security criteria).

Although the standard identifies ISO31000 and ISO/IEC 27005 as providing useful guidance for risk assessment, the organization is in fact at liberty to deploy any appropriate risk assessment methodology that reflects its internal and external context and the requirements of its interested parties. The risk assessment methodology could – but does not need – to be asset-based. It must identify risks, risk owners and risk acceptance criteria, must analyse risks in terms of likelihood and consequence and, above all, must produce 'consistent, valid and comparable results'.

ISO27001 allows flexibility in choice of risk assessment methodology both in order to simplify, for larger organizations, the process of integrating information security risk management with the enterprise-level risk management framework (eg ISO31000) already in place and, for organizations facing specific contractual or market requirements, customer and contractual alignment.

There are a number of risk assessment methodologies – some asset-based, others scenario-based – which might be appropriate for use in an ISMS. We have drawn all those methodologies together into a single, comprehensive guide to risk management, called *Information Security Risk Management for ISO27001/ISO27002* also by Alan Calder and Steve G Watkins (2019). This chapter focuses on the risk assessment methodology contained in ISO/IEC 27005, as it is specifically designed for use within an ISO27001 ISMS.

Risk assessment is a systematic study of the probability and consequences of events, or, alternatively, the systematic and methodical consideration of: 1) the business harm likely to result from a range of business failures; and 2) the realistic likelihood of such failures occurring. Risk treatment (which, with risk assessment, makes up the two stages of risk management) might involve the selection of controls in order to reduce risk to an acceptable level.

The information security risk assessment must be a formal process. In other words, the process must be planned, and the input data (including how existing controls incorporated), their analysis and the results should all be recorded. 'Formal' does not mean that risk assessment tools must be used, although in many situations they are likely to turn a potentially difficult and time-consuming task into one that can be completed in a meaningful timescale and to add significant value. Risk assessments must also produce 'consistent, valid and comparable results'; this requirement (clause 6.1.2.b) tends to support the use of a purpose-developed risk assessment tool (like, for instance, vsRisk™), and a well-defined methodology.

The complexity of the risk assessment will depend on the complexity of the organization and of the risks under review. The techniques employed to carry it out should be consistent with this complexity and the level of assurance required by the board.

You should, at this point, extend your initial glossary of terms to include definitions (all of which should be sourced from ISO27000) of risk, risk analysis, risk assessment, risk evaluation, risk management and risk treatment.

Who conducts the information security risk assessment?

It is entirely up to the individual organization to choose who is to perform this risk assessment, and how. There are two issues to consider before deciding who will do it. The first is that there should be periodic reviews of security risks and related controls – taking account of new threats and vulnerabilities, assessing the impact of changes in the business, its goals or processes, technology and/or its external environment (such as legislation, regulation or society) and simply to confirm that controls remain effective and appropriate.

The second is that the standard requires the organization to identify the competences required of the people operating within the ISMS, including those involved in risk assessment. The need for an appropriately competent person was covered in some detail in Chapter 4. It is essential that risk assessment – the core competency of information security management – is conducted by an appropriately qualified and experienced person. This is logical; the key step on which the entire ISMS will be built needs, itself, to be solid. The ISO27001 auditor will therefore want to see documentary evidence of appropriate knowledge skills.

A number of organizations will already have a risk management function staffed by people with training that enables them to carry out risk assessments. The role of the risk management department is, usually, systematically to identify, evaluate and control potential losses to the organization that may result from things that have not yet happened. The skills and methodology of this department may or may not meet the organization's requirements. Either way, there are potentially significant benefits for such an organization if its information security risk assessments can be carried out by the same function that handles all risk assessments. The benefits lie not just in cost-effectiveness but in the fact that such a risk management or risk control

department will have an existing and ongoing understanding of the business, its goals and environment, and an appreciation of all the risks faced by the business in the pursuit of its objectives. Equally, it should be able to assess how all the different risks, and the steps taken to mitigate them, may be related and coordinated.

Many organizations, however, do not already have an internal risk management function. There are then two possible ways to tackle risk assessment. The first is to hire an external consultant (or firm of consultants) to do it. The second is to train someone internally. The second is preferable in most cases, as the organization 'shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur', and having the expertise in-house enables this to be done cost-effectively. Chapter 4 discusses how to recruit and/or train a specialist information security adviser, and if information security risks are the only ones being considered, then this would be an appropriate person to undertake the risk assessment.

In circumstances where the organization has existing arrangements with external suppliers for risk assessment services, or is in the process of setting up a risk management function or capability (in the context of responding to the requirements of an external risk management requirement, perhaps), then it should from the outset investigate ways in which its risk assessment processes can be integrated.

It is more difficult for a smaller business to retain specialist information security expertise in-house than for a larger one; the internal risk assessment role needs to be maintained over time and the person concerned needs to continue being trained and involved in risk assessment issues, both inside and outside the organization. The disadvantage of hiring external risk assessors, apart from the cost, is that the organization does not necessarily get continuity of involvement from a firm of assessors. The advantage of the external hire, apart from its being a variable cost, is that the external assessor should be up to date on relevant issues and should be wholly objective. A possible middle route is to contract on a multi-year basis, with an appropriately trained individual or consultancy firm to provide risk assessment support and guidance as and when it is required. But however the organization chooses to acquire this resource, it is crucial that a lead risk assessor is in place and fully involved in the risk analysis and assessment process that the rest of this chapter describes.

There are software tools that have been designed to assist in risk assessment, but the use of them is not mandatory. It is essential, though, that the

risk assessment should be done methodically, systematically and comprehensively, producing valid, consistent and comparable results; this means that the process should not be subjective or rely exclusively on the experience and judgement of one or two information security professionals. An appropriate information security risk assessment tool, designed with ISO27001 in mind and kept up to date in terms of changing information security issues, can be effective in this process. vsRisk™, from Vigilant Software Ltd, is one such tool.

Security in any system should be commensurate with its risks. However, determining which security controls are appropriate and cost-effective can be a complex and subjective process. One of the prime functions of security risk analysis is to put this process on to a more objective basis. Most forms of risk analysis involve the use of risk analysis tools, specific to ISO27001, that are designed to ensure that the scope of the exercise is comprehensive and the process rigorous.

There are a number of different approaches to risk analysis. However, these essentially break down into two: quantitative and qualitative.

Quantitative risk analysis

This approach looks at two issues: the probability of an event occurring and the likely loss should it occur. A single figure is produced from these two elements, by simply multiplying the potential loss (measured in monetary terms) by its probability (measured as a percentage). This is sometimes called the annual loss expectancy (ALE) or the estimated annual cost (EAC). Clearly, the higher the number that an event or risk has, the more serious it is for the organization. It is then possible to rank events in order of risk (ALE) and to make decisions based upon this.

The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability is usually assessed subjectively and is rarely precise. In some cases, this approach can promote or reflect complacency about the real significance of particular risks. The monetary value (particularly of reputational damage) of the potential loss is also often assessed subjectively, and when the two components are multiplied together, the answer is equally subjective. When quantitative analysis is done accurately, the time cost of that accuracy quite often outweighs the benefits the organization is able to derive from it.

In addition, controls and countermeasures often have to tackle a number of potential risk, and the risks themselves are frequently interrelated.

A detailed ranking in order of ALE can make it difficult to identify these interrelationships and lead to poor, cost-ineffective decisions about controls, and this approach is not, therefore, recommended. Nevertheless, we do recognize that a number of organizations have successfully adopted quantitative risk analysis.

Qualitative risk analysis

The qualitative approach is by far the more widely used approach to risk analysis and is the approach at the heart of ISO27005. Numeric probability data are not required, and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements, and they are best laid out in tabular form in a corporate risk log, so that, for each asset, its owner(s), threat(s), vulnerabilities and impact(s) are identified.

ASSETS WITHIN THE SCOPE

The first step is to inventory all the information assets (and 'assets' includes processes, information, information systems, hardware, software, etc; control 8.1.1. of ISO27002) within the ISMS scope and, at the same time, document which role and/or department 'owns' the asset, as provided for in control 8.1.2. Although not mandated by ISO27001, asset-based risk assessment is the most sensible approach.

THREATS

Threats are things that can go wrong or that can 'attack' the identified assets. They can be either external or internal to your organization; they are always external to the asset. Examples might include fire or fraud; many such potential threats are described in Chapter 1. Threats are always present for every system or asset; because it is valuable to its owner, it will be valuable to someone else; if it is lost, it would have an impact. If you cannot identify a threat to an asset, you might assume that it is not really an asset.

VULNERABILITIES

Vulnerabilities leave a system, or asset, open to attack by something that is classified as a threat, or allow an attack to have some success or greater impact. For example, for the external threat of fire, a vulnerability could be the presence of flammable materials (eg paper) in the server room. In the language of the standard, a vulnerability (which can be an absence of or

weakness in a control) can be exploited by a threat. The baseline security criteria approach means that, when carrying out a risk assessment, you are looking at risks which exploit vulnerabilities that exist in spite of the controls that are already in place to meet contractual, regulatory and business requirements.

IMPACTS

The successful exploitation of a vulnerability by a threat will have an impact on the asset's availability, confidentiality or integrity – in respect of all or one of the business, contractual or compliance requirements of the business. These impacts should all be identified and, wherever possible, assigned a relative value based on the cost to the organization of that attribute being compromised.

RISK ASSESSMENT

The risks then have to be assessed to identify the potential business harm that might result from each of them. There should then be an assessment of the likelihood of the threat exploiting the vulnerability to create the impact. This enables one to identify the level of risk (and, for smaller organizations, a low–medium–high classification is usually adequate), and this enables one to conclude, for each risk, whether it is acceptable or if, conversely, some form of control is required.

CONTROLS

Controls are the countermeasures for risks. Apart from knowingly accepting risks that fall within the criteria of acceptability, or transferring the risk (through contract or insurance) to others, the ISC^2 Common Body of Knowledge (CBK) describes five types of control:

1. directive controls, which are generally administrative, such as creating policies;
2. preventive controls, which protect vulnerabilities and make an attack unsuccessful or reduce its impact;
3. detective controls, which discover attacks and trigger preventive or corrective controls;
4. corrective controls, which reduce the effect of an attack;
5. recovery controls, which are often associated with business continuity and disaster recovery.

We believe the first of these is actually a way of delivering the second, third and fourth and that the fifth is a subset of the fourth.

It is essential that any controls that are implemented are cost-effective. The principle should be that the cost of implementing and maintaining a control should be no greater than the potential (time-sensitive) cost of the impact. It is not possible to provide total security against every single risk, but it is possible to provide effective security against most risks. However, these can change, and so the process of reviewing and assessing risks and controls is an ongoing one.

The process for assessing risk builds on the scoping exercise discussed in Chapter 5 and should be focused on critical systems and information assets (at least initially; organizations can, if they wish, deal with non-critical systems and assets at a later date). It can be broken down into a number of clearly defined steps:

1. Identify the boundaries of what is to be protected (the scope).
2. Identify the assets: all the systems necessary for the key business processes of receiving, storage, manipulating and transmitting information within those boundaries and the information assets within those systems.
3. Identify the relationships between these systems, the information assets and the organizational objectives and tasks.
4. Identify criticality: identify those systems and information assets that are critical to the achievement of organizational objectives and tasks.
5. Identify the potential threats to those critical systems and assets.
6. Identify the potential vulnerabilities of those critical systems and assets.

Clearly, the combination of the likelihood of the threat exploiting the vulnerability, when combined with the impact on the organization of the asset being compromised, enables the risks that relate to each of the assets to be identified. However, we will first explore each of the steps above in more detail.

Identify the boundaries

It is essential to decide the boundary within which protection is to be provided. The business environment and the internet are each so huge and diverse that it is necessary to draw a boundary between what is within the organization and what is without. In simple terms, boundaries are physically or logically identifiable. Boundaries have to be identified in terms of

the organization, or part of the organization, that is to be protected, which networks and which data, and at which geographic locations.

Identifying boundaries within the Cloud is particularly difficult. The key concept to have in mind is that the scope of the ISMS cannot include elements which are outside the control of management. A Software as a Service (SaaS) product (eg Office365) is outside the organization's control; Microsoft make decisions about how to secure it and their customers can take or leave the consequences. All the client can do is to decide whether or not, on the basis of Microsoft's ISO27001 certification, to trust its data to their SaaS offering.

ISO/IEC 27018 provides an additional set of controls, complementary to those in ISO27002, which are specifically intended for use in Cloud environments, where a data controller contracts with a cloud processor in relation to personally identifiable information (PII). This control set is more broadly useful in helping organizations address security issues in a distributed cloud environment. ISO/IEC 27017 provides an additional generic set of controls for cloud computing services.

Cyber Essentials

This is a useful point to identify the existence of the UK Cyber Essentials scheme. This is an accredited certification scheme that sets out minimum security controls that every organization of any size should adopt in order to protect itself from the majority of low-level but high-volume cyber attacks. Achievement and maintenance of Cyber Essentials certification could be seen as a baseline security control, at the cyber level of fitting doors and windows with working locks; it is increasingly a baseline requirement for contracting with the UK government. The Cyber Essentials scheme works well with ISO27001; read more about it at www.itgovernance.co.uk/iso27001-and-the-cyber-essentials-scheme (archived at https://perma.cc/T4G2-FCSB).

Scope was first mentioned in Chapter 5. The organization that is within the ISMS scope must be capable of physical and/or logical separation from third parties and from other organizations within a larger group. While this does not exclude third-party contractors, it does make it practically very difficult (although not necessarily impossible) to put an ISMS in place within an organization that shares with others significant network and/or information assets or geographic locations. A division of a larger organization that,

for instance, shares a group head office and head office functions with other divisions could not practically implement a meaningful ISMS. Usually, the smallest organizational entity that is capable of implementing an ISMS is one that is self-contained. It will have its own board of directors or management team, its own functional support, its own premises and control over its own IT network.

It is nevertheless possible for divisions of larger organizations to pursue certification independently; the critical factors are the relative independence of management and the extent to which the division can be practically differentiated from other divisions of the same parent organization.

For larger organizations, with a multiplicity of systems and extensive geographic spread, it is as a general rule often simpler to tackle ISO27001 and, in particular, risk assessment on the basis of smaller business units that meet the general description set out above. Larger organizations that have a single business culture and largely common systems throughout are probably better off creating a single ISMS.

Once the organizational scope is identified, it is necessary to list the physical premises that the chosen organization occupies and to identify its network and information assets. The implementation team should list these, but should only do it at this point at the highest possible level.

Identify the assets

Assets are discussed in more detail in Chapter 8. Primary assets are the key business processes and information. Key information assets may have be either information systems or bodies of information. A system consists of a number of components. A single data asset (such as a file, whether electronic or paper) is a component of a system. At this stage, we are concerned only with the systems, although at a subsequent point it may be necessary to analyse vulnerabilities down to the individual data asset level.

These systems will include a number of IT systems, consisting of software (eg client relationship management system, payroll system, e-mail system, resource planning system, accounting system), hardware (eg servers, workstations, routers), telecommunications systems and paperwork filing systems. The implementation team should list the key systems and their components throughout the organization. There are software tools that can be used to ensure that all the data assets and all the IT systems have been identified, and these are discussed later.

Telecommunications systems will include mobile phones as well as desk-based systems; smartphones are as important a component of the IT system

as are the remote access points and subcontracted services. Critical paper filing systems are as important as digital folders and drives. All the systems need to be identified, and if, in the process of doing this, there are found to be significant sharings of assets or information sharings that were not identified earlier, then the scope of the ISMS may need to be revisited.

Individual items should be grouped by similarity of item type and exposure to risk. The sales teams laptops could, for instance, be treated as a single asset group: they all do the same thing, have the same value to the organization and are exposed to the same range of threats. Every asset has an owner, and for the risk assessment to be useful it is necessary to identify (by position, rather than name) the individual who owns – who is accountable for – each information asset.

Identify criticality: the relationships between assets and objectives

The key objectives (which may have business, contractual or legal aspects to them) should be identified in the organization's business plan. Of course, if they are not, then this is a good opportunity for senior executives to identify and agree the key objectives of the organization and to map the tasks necessary to deliver them.

Objectives are often expressed as being to do with increasing market share, or increasing profitability, or increasing margin. These, however, are really the outcomes of pursuing operational objectives such as 'sell more of product X to customer type Y'. There will be a hierarchy of objectives that reflects the value that the organization places on the outcomes that their achievement will deliver. There will also be a number of underlying objectives, which are really business requirements (the activities that are considered important for the ongoing effective operation of the organization). 'Comply with the law' is likely to be such an objective and will be common to most organizations.

Organizational business plan objectives should, like all objectives, be SMART (specific, measurable, achievable, realistic and time-bound). The key objectives should be clearly documented and this, or an excerpt from the business plan in which they are identified, should form part of the ISMS records.

Once the key objectives are clearly identified, then those systems that are most important to their delivery can also be identified. This is best done by the whole implementation team in a single session (which, depending on the size of the organization, may take one or more days) with lots of flipcharts. The starting point, after agreeing the scope of the planned ISMS, should be

to brainstorm a list of all the systems used within the business, whether digital or not. The team can then move on to review and understand the business objectives and then identify the relationships between systems and objectives.

The objective is to reach a conclusion that reflects all members' experience and knowledge; that identifies all the systems and in which all the business objectives have their critical system dependencies identified. It is possible that some objectives will have more than one system, and these interdependencies should also all be noted. Note that external consultants could only achieve this objective through a facilitated workshop or an extensive series of one-to-one interviews. It is important that the whole range of experience, perception and prejudice is involved in the process at this time, as otherwise it is likely that key dependencies may be missed or misconstrued.

It usually makes sense, in this same session, to move straight on to ranking the systems in order of critical priority – taking into account the business, contractual and legal requirements – to the business. This tends to be the best way to take full advantage of the momentum generated in the first session and ensures that the fullest possible analysis of the priorities is carried out. Meaningful ranking will depend, of course, on the effectiveness of the earlier analysis and ranking of business objectives.

The resulting report, a schedule that shows critical systems as dependencies of key organizational objectives, should be reviewed and agreed by the senior management team of the organization. It is critical that there is the fullest possible agreement on this, as this will be a key building block of the ISMS. The whole process set out above should be fully documented.

It is worthwhile, in tackling this (and the tasks below), to adopt an approach that is pragmatic, questioning and transparent. By this, we mean that the risk assessment should be done, and driven, by human beings – it is a subjective exercise in an environment where returns are derived from taking risks – and that it is preferable to be 'approximately correct, rather than precisely wrong'. All individual inputs will reflect individual prejudice; the process of gathering input should question this input to establish what is known – and what unknown – in the individual assessment.

It is now possible to assess the impact on the organization of confidentiality, integrity and availability for each of the identified assets. Broadly speaking, impacts will fall into one (or more) of three damage categories: damage to the organization's business (its competitive position, its finances and its reputation), to its contractual commitments or to its legal responsibilities. The project team should identify the nature of each impact.

The next step is to assess the extent of the possible loss for each potential impact. One object of this exercise is to prioritize treatment (controls) and to do so in the context of the acceptable risk threshold; it therefore makes sense to categorize possible loss rather than attempt to calculate it precisely. The categories of business loss (for a large organization) might be:

None	Losses are between nil and £10,000
Minor	Losses would be above £10,000 but lower than £50,000
Medium	Losses would be above £50,000 but lower than £100,000
High	Losses would be above £100,000 but lower than £1 million
Very high	Losses would be above £1 million and lower than £10 million
Extreme	Disastrous – the financial viability of the organization is threatened

The financial equivalents provided above should be adjusted, under the board's guidance, to levels appropriate to the size of the organization and its current risk treatment (or enterprise risk management) framework. In assessing the potential costs, all identifiable costs – direct, indirect and consequential – including the costs of being out of business, should be taken into account. The 'better to be approximately correct than precisely wrong' approach should continue to be deployed in this exercise.

Identify potential threats and vulnerabilities (likelihood)

For each of the assets on the schedule, it is now necessary to identify the possible vulnerabilities and the potential threats to the key business systems. There are a high number of threats, and the range of possible vulnerabilities is also substantial. The input of the trained information security expert is, at this point, invaluable and the guidance of ISO27005, which includes lists of threats and vulnerabilities, can also save time. Threats tend to be external to the systems (but not necessarily to the organization). They include hostile outsiders such as hackers, non-hostile outsiders such as suppliers or cleaning contractors, and insiders, both the disaffected and the committed but careless, or even just the poorly trained. Vulnerabilities are security weaknesses in the existing systems, weaknesses that can be exploited by threats, or that allow one or more of the confidentiality, integrity and availability of the asset to be compromised, accidentally or otherwise. A vulnerability can also simply be the absence of a control or a weakness in its implementation.

It is necessary to consider the links between threats and vulnerabilities. An example might be cleaning contractors who inadvertently pick up (a minor threat, being the unintentional error of a third party) the only copy of

an extremely confidential document off an executive's desk (a minor vulnerability, the forgetfulness of an executive) in the ordinary course of cleaning, and dispose of it. At this point, only the availability of the data has been affected, and the repercussions might be minor, as it might be possible – if embarrassing and time-consuming – to recreate the document. However, once an industrial espionage operative rummaging through the waste sacks of the organization finds the document and makes it available to the organization's competitors, the confidentiality of the information will have been compromised and the cost to the organization of the security breach starts increasing dramatically.

A telephone system that crashes, losing all stored voicemail, could have a significant impact on any organization that relies on voicemail for sharing critical information. Such an organization needs to have thought through how it will manage the security of these data.

Inevitably, the exercise to identify threats and vulnerabilities to the systems cannot be carried out without also identifying vulnerabilities in systems, and impacts on the organization, that are not necessarily threats to the availability, confidentiality or integrity of its information, but to which there is nevertheless a significant cost. An example is in digital telephone systems that enable direct-line users to access their voicemail externally and to redirect calls. The evident threat to data confidentiality is that unauthorized users could access information stored in voicemail. If voicemails can be deleted externally, then there is the threat that unauthorized users might make information unavailable. In addition, an unauthorized user could be able to use the organization's telephone number to forward calls to his or her own number anywhere else in the world, or even to dial from the extension to anywhere else in the world.

Essentially, threats for each of the systems should be considered under the headings of threats to confidentiality, to integrity and to availability. Some threats will fall under one heading only, others under more than one. It is important to have carried out this analysis systematically and comprehensively, to ensure that no threats are ignored or missed. The effectiveness of the controls that the organization eventually implements will reflect the quality of this particular exercise.

Many external threats will be classified under all three headings. A hacker might be able to steal confidential data and then disrupt the information system so that data are no longer available or, if they are, they are corrupted. A virus can affect not only the integrity and availability of data but also, because it could mail out a copy of an address book, confidentiality as well.

A business interruption, such as a fire in a data centre or a filing cabinet, is likely to affect the availability and integrity of information.

Similarly, what is likely to be a threat to one system is not necessarily a threat to another. For example, a fire in the server room is a threat to a number of systems based there, but is unlikely to be a threat to an organization's mobile phone network.

The penultimate step is to assess the probability or likelihood of each impact occurring. The probabilities that might be used are:

Negligible	Unlikely: less than once every five years
Very low	Likely to occur less frequently than once per year but more frequently than once every five years
Low	Likely to occur more than once every year but less than once every six months
Medium	Likely to occur more than once every six months but less than once every month
High	Likely to occur more than once every month but less than once every week
Very high	Likely to occur more than once every week but less than once every day
Extreme	Likely to occur at least daily

Create a risk matrix, using the scales you have created, that has likelihood along one axis and impact along the other. The risk acceptance criteria can be represented on the matrix by means of mapping then blocking out the levels of likelihood and impact that managers consider acceptable. For each threat–vulnerability combination, you can the plot the risk level onto this matrix by plotting the intersection of the likelihood and impact. Any risks that fall outside the organization's risk acceptance criteria must be treated.

The final step in this exercise is to transfer the risk level assessment for each impact to the risk log. Although the examples we have used are based on five levels, we suggest that – particularly for smaller organizations – three levels of impact and likelihood are usually adequate: low, moderate and high. Where the likely impact is low and the probability is also low, then the risk level could be considered very low; where the impact is at least high and the probability is also at least high, then the risk level would be very high; anything between these two measures would be classed as moderate. However, every organization has to decide for itself what it wants to set as the thresholds for categorizing each potential impact.

Selection of controls and Statement of Applicability

The standard, at clause 6.1.3, requires the organization to select appropriate information security risk treatment options and then determine all the controls necessary to implement the selected treatment. 'Organizations can design controls as required or identify them from any source.' This does mean that the organization is at liberty to deploy any appropriate control set (typically driven by internal and external context and the requirements of interested parties). Appropriate control sets could include those from PCI DSS, NIST, COBIT, Cloud Security Alliance or, of course, ISO/IEC 27002 and the related ISO27000 family of standards. ISO 27017 and ISO 27018 tend to be particularly popular for those organizations operating in the cloud, and processing personally identifiable information in the cloud.

The selected controls are then compared with those listed in Annex A of ISO27001, and the organization produces a Statement of Applicability which identifies, with justifications for both inclusions and exclusions, which Annex A controls have been selected, and which additional controls have been selected. In addition, the SoA should identify which of the selected controls have actually been implemented. Annex A is, in this sense, a referent control set, which enables organizations to ensure that they have not missed any relevant controls. This book proceeds on the basis that the Annex A/ISO27002 control set has been selected.

ISO27002 provides best practice guidance on the implementation and operation of the controls listed in Annex A. There may, however, be some areas in which organizations may need to go further than is described in ISO27002, and the extent to which this may be necessary is driven by the extent to which technology and threats evolve after ISO27002:2013 was published.

Controls are selected in the light of a control objective. A control objective is a statement of an organization's intent to control some part of its processes or assets and what it intends to achieve through application of the control. The selection of controls should be cost-effective, which means that the cost of their implementation (in cash and resource deployment) should not exceed the potential impact (assessed in line with our discussion above) of the risks (including safety, personal information, legal and regulatory obligations, image and reputation) they are designed to reduce.

It is important that, when considering controls, the likely security incidents that may need to be detected should be considered and planned for. In

effect, the process of selecting individual controls, whether from Annex A or elsewhere, should include consideration of what evidence will be required: 1) to demonstrate that the control has been implemented and is working effectively (the measuring of effectiveness is addressed at the end of this chapter); and 2) that each risk has thereby been reduced to an acceptable level. In other words, controls must be constructed in such a manner that any error, or failure during its execution, is capable of prompt detection and that planned corrective action, whether automated or manual, is effective in reducing to an acceptable level the risk of whatever may happen next.

Annex A of the standard has 14 categories, each of which has a number of subsections. There are, in total, 114 controls, each of which has a four-component alphanumeric control number. Each needs to be considered and a decision made as to whether or not it is applicable. As the controls are selected, the Statement of Applicability (SoA) can start to be drawn up. This SoA, specified in 6.1.3.d of the standard, is documentation of the decisions reached against the previous requirement and also an explanation or justification for the selection or non-selection of the controls that are listed in Annex A and whether or not the control has been implemented. This document needs to be reviewed on a regular basis and will be one of the first documents that the external auditor will want to see. It is also the document that is used to demonstrate to third parties the control framework that has been implemented, and is referred to, with its issue status, in the certificate of conformity issued by third-party accredited certification bodies.

The SoA could form the core of an ISMS manual or adopt the format set out below. The wording provided in the standard is repeated with appropriate variations to reflect the actual decisions made by the management steering group and its reasoning. The SoA can also refer to other documents, where these form the basis for any specific decisions recorded in it or which implement the decisions described. There are different ways of expressing the way in which different controls are applied, some of which are in the example below. The SoA should be signed by the owner of the ISMS (likely to be the CEO) for which it has been drawn up. This document is, for the external certification auditor, key evidence of the steps taken between risk assessment and implementation of appropriate controls.

The fact that someone reviewing an ISO27001 certificate might ask to see the SoA referred to should point at an appropriate level of classification; realistically, a standalone SoA that doesn't contain any sensitive security information is a practical solution.

Statement of Applicability Example

Introduction

This is the SoA, as specified in clause 6.1.3.d to ISO/IEC 27001:2013 ('the Standard'), for ABC Ltd. It was adopted by the Management Steering Group on [date] and will be reviewed in the light of significant information security incidents and at least annually. It reflects a risk assessment carried out on [date]. Controls are addressed in the same order and using the same numbering as in Annex A of the Standard, and this statement explains which controls have been adopted and identifies those that have not been adopted and sets out the reasons for non adoption. All of the adopted controls have been implemented.

Statement of Applicability

A.5.1.1 Policies for Information Security
ABC Ltd has adopted this control in order to meet business and contractual requirements

A.6.1.2 Segregation of Duties
ABC Ltd has adopted this control in order to meet regulatory requirements

A.6.2.2 Teleworking
ABC Ltd has not adopted this control as it has no teleworking sites

As we indicated earlier, some thought needs to be given to the circulation of your SoA: it will be referenced on the certificate awarded following a successful audit to ISO27001, and so anyone who knows anything about ISO27001 certification will want to see a copy of the SoA as well as the certificate (and any other documents describing the scope, but this is normally stated on the certificate in its entirety). This suggests that the SoA will need to be a public document.

A catch could be that the complete SoA might include references to assets that the controls relate to and/or the ISMS documents that give life to the controls, and may have content in it that needs to be kept away from 'public' consumption. Those customers or other third parties who require sight of the SoA in order to establish the nature of the ISMS would therefore have to enter into a non-disclosure agreement before they could do so. This leads some organizations to produce two versions of their SoA, a limited version

for public consumption and a comprehensive version for internal or controlled use only.

For example, with the following SoA table (Table 6.1), the version containing the white columns could be made available publicly and access to the complete version that includes the shaded columns could be restricted. The 'applied' column provides for 3 options: yes and implemented; not selected.

TABLE 6.1 Statement of Applicability (SoA) table

Control		Applied Y/YA/N	Justification
Reference	Description		
A.5.1.1	Infosec policies	Y	Required by ISO 27001 with additional policies required as a result of the information security risk assessment
–	–	–	–
–	–	–	–

This book will explore each of the controls listed under Annex A, looking to the good practice set out in ISO27002 for how best to implement them. The book will (mostly) tackle the controls in the order laid out in the standard; the organization should, however, tackle and implement controls in the order of priority identified through the baseline security criteria, the risk assessment and the risk treatment plan. The controls that are most critical for the organization will be those that relate to the threats and vulnerabilities that it has identified, through the risk assessment process, as being most serious to its most critical systems and/or information.

Gap analysis

As we said earlier, the reality is that most organizations that embark on ISO27001 already have a number of information security measures in place; ISO27001 necessitates ensuring that those controls that are in place are adequate and appropriate and that additional required controls are implemented as quickly as possible. In other words, an analysis of the gap between what is in place and what might be required might be carried out

could be a useful point of reference when carrying out the risk assessment; bear in mind, as well, our comments about the need for the management system as a whole to work to deliver the information security objectives.

The SoA will be complete once all the identified risks have been assessed and the applicability or otherwise of all the Annex A controls has been considered and documented. Usually, the SoA is started before any controls are implemented, and completed as the final control is put in place.

Risk assessment tools

There is a small number of software tools available that can, to a varying extent, automate the risk assessment process and generate the SoA. In theory, such a tool ought to encourage the user to perform a thorough and comprehensive security audit on the organization's information systems, and ought not to produce too much paperwork as a result. Tool availability is likely to change as the Standard is more widely taken up, and any organization interested in pursuing this route should therefore do up-to-date research on what is available before making a shortlist. This book's website contains information on available tools, including VS Risk™, from Vigilant Software Ltd.

The organization will need to compare tools before making a selection and should concentrate, in the comparison process, on the extent to which the tool really does easily and effectively automate the risk assessment and SoA development process; the amount of additional paperwork it generates; the flexibility it offers for dealing with changing circumstances and frequent, smaller-scale risk assessments; and the meaningfulness of the results it generates. Of course, normal due diligence should also be done into the status of the supplier and manufacturer of the product to ensure that it is properly supported and likely to continue to be. References might also be sought from happy customers.

Risk assessments can, with difficulty, be done without using such tools. A thorough risk assessment, using a manually created spreadsheet for instance, for any significant business will be very time-consuming, and even more so if a software tool is not used. 'Time-consuming' means up to three months, or even longer for larger organizations. The use of a software tool will depend on the culture of the organization and the preferences of the information security adviser and manager. Practically speaking, once the organization has decided to purchase such a tool, it becomes dependent on that tool and on the staff members who are trained to use it. In considering

the appropriate route forward, consideration should be given to the speed with which incoming staff can become familiar with the chosen risk assessment tool; practicality and ease of use are likely to be key attributes.

If the organization decides to purchase such a tool, the steering group should document the reasons for its choice and selection; whoever is to use it will, of course, have to be appropriately trained in its use. Evidence of this training and level or proficiency achieved should be retained on the relevant HR file.

Risk treatment plan

Clause 6.1.3.e of the standard requires the organization to 'formulate an information security risk treatment plan'; this should identify the appropriate management action, responsibilities and priorities for managing information security risks. Clearly, the risk treatment plan needs to be documented. It should be set within the context of the organization's information security policy and it should link clearly to the documents which set out the organization's approach to risk and its criteria for accepting risk, as discussed earlier in this chapter. The risk assessment process must be formally defined, and responsibility for carrying it out, reviewing it and renewing it formally allocated. At the heart of the risk treatment plan is a detailed schedule that shows, for each identified risk, how the organization has decided to treat it, what controls are already in place (the baseline security controls), what additional controls are considered necessary, and the time-frame for implementing them. The gap to the acceptable risk threshold needs to be identified for each risk, as well as the risk treatment option that will bring the risk within an acceptable level.

ISO27001 imports the enterprise risk management concept of a Risk Owner into information security management. At 6.1.3.f, the Standard says that the Risk Owner must approve the risk treatment plan and accept any residual risk. The risk owner could be top management as a whole, or it could be an individual line or functional manager, as the organization considers appropriate. What matters is that the risk owner role is clearly allocated (and in line with clause 5.3), understood and effective, and that the risk owner's formal approval for the RTP, and any residual risk (the risk left over after treatment) in respect of those risks for which they are responsible – is documented.

The Risk Treatment Plan may identify controls that are to be deployed in the future, whether for financial or operational reasons and, as long as the risk owner formally accepts the interim residual risk, this is a practical approach. It may also be that the treatment plan requires a series of actions at different times, with different priorities; a sensible RTP will define the timelines, responsibilities and dependencies.

The risk treatment plan links the risk assessment (expressed in the corporate information asset and risk log) to the identification and design of appropriate controls, as described in the SoA, such that the board-defined approach to risk is implemented, tested and improved. This plan should also ensure that funding and resources for implementation of the selected controls are adequate, and should set out clearly what these are. The risk treatment plan should also identify and consider the individual competence and broader training and awareness requirements necessary for its execution and continuous improvement.

We see the risk treatment plan as the key document that links all four phases of a Plan–Do–Check–Act (PDCA) cycle for the ISMS. It is a high-level, documented identification of who is responsible for delivering which risk management objectives, of how this is to be done, with what resources, and how this is to be assessed and improved; but at its core is the detailed schedule describing who is responsible for taking what action, in respect of each risk, to bring it within acceptable levels.

The risk treatment plan is a living document. As new risks are identified, old risks change, or improvement opportunities identified, the risk treatment plan needs to be updated. The organization needs, therefore, to have a managed process in place that ensures that revised (or new) risk assessments feed through to a revised risk treatment plan and that, where appropriate, changes are signed off by the risk owner.

Measures of effectiveness

ISO/IEC 27001:2013 requires, in clause 9.1, the organization to evaluate information security performance and the effectiveness of the ISMS. One aspect of this is to measure the effectiveness of controls (or groups of controls); controls are implemented to achieve a control objective, the control objectives are linked to the objectives for information security and, therefore, the effectiveness of each control contributes toward the overall effectiveness of the ISMS.

Measures of control effectiveness are ideally agreed during control selection, but this can also be done later. In a sense, the structured decision process required by the risk assessment methodology, and the fact that controls are selected by objective, means that it is reasonable to deduce that if a prescribed control is fulfilling its objective (ie to reduce the predicted risk to the acceptable level) then it is being effective. In designing measures of effectiveness, there are three questions that must be answered:

- What is the objective of each control?
- How can you determine if the control is being effective?
- What are the parameters that will give a positive or negative indication of control effectiveness?

ISO/IEC 27004 provides guidance on measuring control and information security management effectiveness.

Monitoring of measures of effectiveness can be particularly resource-intensive and so it is worth considering, at the point of selecting the controls, the basis on which the measures of effectiveness will be selected and monitored. A certification auditor would find it hard not to accept the selection of monitoring measures based on the largest risk areas, or in relation to those controls that have the biggest positive effect on reducing residual risk, and those should be reported to senior managers at the management review.

ISO27001 is an outcome-orientated management standard. It is a clear requirement of the standard (at clause 6.2) that the organization must monitor the performance of cti ISMS against its objectives; this is key demonstrating, to top management and interested parties, the effectiveness of the ISMS. All the principles of good performance management hold good when applied to information security and measuring the effectiveness of the ISMS and controls. In particular:

- Over-reliance on negative reporting is likely to result in flawed measures.
- Automated monitoring is preferable to manual arrangements.
- The exact aspect being measured needs to be aligned with the main objective.
- The integrity of the measures or statistics being produced is of paramount importance, as management decisions are likely to be based on this information.

7

Mobile devices

Mobile devices and teleworking

Control objective A.6.2 of ISO27002 is to ensure information security when mobile or when working remotely. The protection required should, of course, be proportional to the risks identified (through a risk assessment). Many of the issues related to both mobile working and teleworking have been touched on elsewhere in this book. These include issues around information classification (Chapter 9), equipment security (Chapter 16), virus control (Chapter 18) and access control (Chapter 11). The two sub-clauses deal, respectively, with mobile computing and teleworking.

Mobile computing

Control 6.2.1 of ISO27002 says the organization should have in place a formal policy and appropriate controls to protect against the risks of working with mobile computing facilities, particularly in unprotected locations. If the organization has a BYOD ('Bring Your Own Device') policy, this is where it would primarily occur within the ISMS.

Any organization that operates a mobile computer network – and a Blackberry or smartphone network would count – should take specific steps to protect itself. These controls may also be relevant in respect of staff accessing organizational assets from their own private mobile devices. If it also has teleworkers, this policy for mobile computers could be integrated with that for the teleworkers. The first step is to design and adopt, within the ISMS, a mobile computing policy, which must be accepted in writing by those who wish to use mobile facilities before they are allowed to. The sensible organization will also ensure that users receive appropriate training before they are issued with mobile computing equipment (notebooks, smartphones).

This policy should consolidate all the procedures discussed elsewhere in this manual in respect of mobile computing and handheld usage. It should set out clearly the requirements for physical protection, access controls, cryptography, back-ups and malware protection. It should include clear guidance on how to connect to the organizational network and how mobile tools should be used in public places. 'Public places' include meeting rooms outside the organization's own secure premises and wherever notebooks and handhelds remain tempting targets for hackers and thieves, who can have as much impact on the availability of data as a particularly virulent virus. Guidance on where mobile devices may be used, and for what purposes, should also be provided, with due consideration being given to who may be able to see or hear what is being 'processed'.

The organization will need to develop an effective method of ensuring that anti-malware protection is completely up to date on mobile computers (which are also known as 'endpoints', reflecting the reality that for many networks, it is the notebook and mobile devices that exist beyond the secure corporate perimeter that are the endpoint for corporate security activity). This is best done by using an automatic update service that updates all computers the moment they log on to the organizational network. It is important that the mobile user is not given any authority to override this update and is not able to proceed until the update is complete. This principle should extend to ensuring that the software is fully patched, with all service packs installed; it is not unknown for someone whose primary use of a laptop is for e-mail to avoid actually logging on to the system for months on end, with the consequence that many patches and service packs are not installed. End-point security products have emerged to deal with these specific issues.

Where remote users access organizational facilities, strong authentication should be used, which makes use of strong protocols. Consideration should be given to authenticating the machine as well as the user to provide for the situation where a notebook has been stolen and the user authentication information compromised. The situations where this will be necessary should be identified through the risk assessment.

Back-up procedures (using, for instance, web-based data back-up services) are very important; unlike the requirement that should be in place for computers on a fixed network (no data stored on the C: drive), mobile computers may have all their data stored on the C: drive. The requirement for regular individual back-ups, together with a workstation configuration that automatically backs up the 'My Documents' folder to the main server

when a laptop is logged on to the network (over an appropriate connection), combined with a requirement that any physical back-up media are appropriately protected from theft, loss or degradation (issue protective, lockable boxes), is essential.

Physical security (ensuring that unattended notebooks are locked away and/or fitted with security locks and that notebooks with sensitive information are encrypted and are never left unattended) is an equally important component of an effective mobile computing policy. Given the ridiculously high number of laptops and smartphoness that are lost, stolen or otherwise go missing every year, organizations need to develop specific reporting and recovery procedures based on a risk assessment that includes any legal or insurance issues that may be relevant to the organization. Users should be physically trained in how to do these and should demonstrate that they know how to before they are released into the world with a notebook or handheld.

The proliferation of wireless networks, wireless networking facilities and public wireless access spots has brought a new dimension to mobile computing security. The fact that an individual can access a public wireless network (from, for instance, an airport lounge or a coffee shop) is both extremely convenient and potentially very dangerous. It can be more dangerous than accessing the internet through a fixed link, in that a wireless computer is broadcasting information to the wireless access point – and, therefore, all that information is available to anyone who is interested in it.

A widely deployed security standard deployed on laptop computers is still (Wired Equivalent Privacy). It does not give the privacy of a wired equivalent; it is insecure, and there are many websites that provide information on its inadequacies and how to attack WEP, to decrypt current traffic, to inject new unauthorized traffic or, ultimately, to access the laptop itself. The default configuration for laptops should be that WEP is switched off. It is just as important to secure laptops that may use public access points to access corporate networks; WPA (preferably WPA2) and VPNs should be part of the basic security configuration.

It is essential that before any laptops are issued to mobile users, the organization carry out a risk assessment, and deploy those technological controls (which themselves are evolving quickly) that are most likely to minimize the threat to the organization arising from wireless vulnerabilities.

Increasingly, mobile phones and smartphones are falling within the category of information processing devices that this section is designed to address, and they should therefore, as previously indicated, also be subject

to appropriate controls determined as the result of a risk assessment. Clearly, consideration needs to be given to the logical boundaries between organizational data and the systems, software and Apps on smartphones, which takes us back to the BYOD issues identified earlier.

Teleworking

Control 6.2.2 of ISO27002 says the organization should develop policies, operational plans and procedures to authorize and control teleworking activities. Where the organization has both teleworkers and mobile workers, the two policies should be integrated. Teleworking has increasingly become an extension of mobile working, rather than being simply one or a few workers based outside the organizational perimeter and accessing the network from time to time. The only significant difference between the two is that teleworking involves a fixed base and fixed connection to the organizational network; more information and more extensive facilities tend to exist in the teleworking location. The location itself, usually an employee's home, does not have anything like the physical security that might be available in the workplace and is also vulnerable to domestic thieves.

There are particular controls that should be considered for teleworkers, and these should reflect a risk assessment and be incorporated into a formal policy within the ISMS. The teleworker should be required to sign a suitably modified version of the access agreement discussed in Chapter 12. A NIST publication, *Security for Telecommuting and Broadband Communications*, SP 800–44, available from the NIST website (https://csrc.nist.gov (archived at https://perma.cc/Z5WL-42XB)), is designed to help system administrators and users tackle the information security issues around these areas, and while written for a US audience, it is of value elsewhere. There are also issues of health and safety that will need to be considered, but these are outside the scope of this book.

The risk assessment should consider specific issues in relation to remote locations. Where the organization has a substantial number of teleworkers (eg staff working from home, either permanently or infrequently but regularly), it might consider a standardized form of risk assessment that looks for exceptions to minimum requirements, can be carried out at a distance and depends on employee information for completion. This input should be subject to random physical checks. If the system is too complex and

time-consuming to set up, the benefits to be gained from teleworking will be outweighed by the work it requires to set someone up.

A key issue to consider, for teleworkers, is the physical security of the site. The organization should look at the physical security of the proposed building (usually a house) and also take into account the security of the surrounding area. The teleworking environment within the building should also be considered: is it a separate office or is it in a communal area? The communications requirement should be assessed; this should take into account the information classification, the underlying linking technology and the sensitivity of the system to which it links. Lastly, the threat of unauthorized access to the facilities (including from family and friends) should also be assessed.

There are a number of controls that might be considered and that should be included in the teleworking policy. As with the mobile working policy, teleworkers should not be authorized to start activity until they are satisfactorily trained. The controls should include provision, by the organization, of suitable and adequate equipment and appropriate furniture that make storage and proper usage possible. Consideration should be given to printers, files, peripheral drives and safety equipment such as anti-glare screens and wrist rests that might be available in the workplace. Full-size screens, keyboards and mice might also be appropriate.

The permitted work should be defined, including the hours of work and the classification of information that may be held at, or accessed from, the location. The organizational systems and services that the user is authorized to access should also be described. Appropriate communication equipment should be provided (internal modem, ISDN, ADSL, broadband, etc, depending on communication needs, available technology and the cost–benefit analysis), and how secure remote access is ensured must also be decided. Physical security – how the equipment is to be protected against breakage and theft – is as important as the establishment of appropriate insurance cover for it (it should not be left to the employee to organize cover under a household policy, as this will usually not be applicable). There should be rules about what access families and friends can have to the facilities and to the equipment. Critically, these must take into account any other devices that may run on a home network and any wireless devices or wireless networking. Appropriate steps should be taken to provide hardware and software support and maintenance; usually this includes an extended service from the organizational helpdesk staff, whose hours will need to be extended

to cover home working and whose skills will need to encompass their peculiar problems.

There are specific issues that will need to be addressed if the teleworker is going to use privately owned equipment. One such issue could be that of ownership of business ideas or intellectual property developed on privately owned equipment either during or after working hours, and this issue should be addressed (depending on the risk assessment) with the help of the organization's professional legal advisers; appropriate clauses, which should also cover dispute resolution, should be inserted into the teleworker's access agreement. Other issues specific to privately owned equipment include the need for the organization to access the equipment (either to check security or as part of an investigation); software licensing agreements consequent upon the deployment to a private machine of organization-specific software; and requirements about the level of firewall and anti-malware protection. Like the IP issue, these should all be addressed in the light of a risk assessment and with professional advice that informs the teleworker's access agreement.

There should be clear rules about back-up, anti-malware and continuity plans, with appropriate resources provided to make this as easy as possible. It should be borne in mind that the risks to the organization are greater in relation to individual teleworkers than in relation to individual users on the organizational network.

Teleworkers should certainly be subject to audit and monitoring just as for any other person attaching to the network, and there should also be a documented process for revoking general or specific teleworking authorizations and to ensure that all equipment is returned.

8

Human resources security

Clause 5.1 of the standard requires the organization to ensure that the resources needed for the ISMS area available and clause 7.2 requires that that whoever is assigned an ISMS-related task has the necessary competence. The HR aspects of two clauses can be satisfied at the same time as the relevant HR controls are implemented.

Clause 7.2, in particular, requires the organization to determine what competences are necessary for those doing work within the ISMS, and then to ensure (by assessment and evaluation) that these persons are actually competent, providing relevant education, training or experience, and to keep appropriate documentary evidence. Note that 'persons doing work under organization's control' can extend to volunteers, associates and contractors as well as full-time employees.

Section 7 of ISO27002 is structured to deal with human resources security in a way that covers the three stages of employment: pre-employment, during employment and post-employment. Control 7.1 of the standard deals with pre-employment security issues. The objective of this clause is to ensure that employees and contractors are suitable for their roles, and understand their information security responsibilities. Control 7.1.1 deals with pre-employment screening, and 7.1.2 deals with contracts and roles and responsibilities in respect of the ISMS and information security within the organization. This should include both *general* and *specific* responsibilities.

Job descriptions and competency requirements

Every job description should contain: 1) a description of the competencies required for the role; and 2) a statement to the effect that every employee is required to be aware of the organization's policy on information security

(a copy of the policy might be attached to the job description) and to take whatever actions may from time to time be required of him or her under the terms of the organization's ISMS. In particular, the employee's attention should be drawn to the responsibility to protect assets from unauthorized access, disclosure, modification, destruction or interference, the information classification and handling rules, the access controls (both physical and logical), the incident reporting procedure, the requirements to carry out any other specific procedures and processes, the requirement personally to improve competence and skills in this area, and the fact that the employee will be held accountable for his or her acts of commission and omission. The job description should set out clearly that breach of information security controls may be considered a misdemeanour under the organization's disciplinary policy and that breach of them might, under specific circumstances, result in dismissal.

Specific requirements should in addition be included in the job descriptions of particular individuals. If the organization prefers not to identify required competencies for *all* roles, it will at least be necessary to do so for those involved in the ISMS. The people who should be considered for such specific requirements include:

- the chief information and/or the chief information security officer;
- the information security adviser;
- members of the information security management forum;
- IT managers;
- network and website managers;
- IT, website and helpdesk support staff;
- premises security staff;
- HR, recruitment and training staff;
- general managers;
- finance staff;
- the company secretary and legal staff;
- the business continuity and emergency response team.

People in each of these functions (and there are likely to be others – each organization is different and each organization needs to make arrangements that are appropriate to it) are likely to have a direct impact on the effectiveness of implementation of the information security policy and the ISMS.

While Chapter 4 contained an initial discussion of the generic responsibilities that apply to particular functions, the only effective way to ensure that all information security responsibilities are captured will be for the members of the information security management forum to work through all the clauses of the standard, identifying which members of staff will be responsible for implementing the clause or will be affected by it. These responsibilities should then be included in the job descriptions for these people.

This analysis should be underpinned by a review of all the roles, functions and employment levels of staff within the organization; this review should consider what responsibility, if any, people in given roles will have in ensuring the confidentiality, integrity and availability of information in the organization. The conclusions of this review should be compared with those generated by the analysis carried out on the basis of the clauses of the standard. A statement of information security responsibility that combines both outputs should then be the final form of the amendment to the job description.

This statement of information security responsibility could either have a separate headlined and complete paragraph in the job description, in which case the member of staff affected should sign and date a copy of the amended job description, or there should be a separate statement attached to the job description and referred to in the job description, in which case both documents should be signed and dated by the employee. The signed document should then be retained on the individual's personnel file.

As part of any arrangements with third parties that involve their access to the organization's information assets, security roles and responsibilities that match those required by the organization should be implemented by the third party and appropriately monitored by the organization.

Screening

Control 7.1.1 of ISO27002 deals with verification checks on permanent staff and contractors at the time of job applications. The organization should identify who will be responsible for carrying this out, how it will be done, how the data will be managed and who will have what authority in respect of the data and the recruitment process. Any screening and data collection activity must be carried out in accordance with the relevant local legislation. There is, in some roles, a legal requirement to carry out criminal screening, and there are clearly risks in taking unknown staff into the organization, not just in terms of fraud and confidentiality but also in terms

of integrity and availability. An inadequately experienced IT staff member could mismanage a vital server or application in such a way that information availability and integrity are compromised. This clause provides more information about the type of verification envisaged. It sets out five basic checks that should be completed:

1. Character reference checks, one personal and one business. These should, for preference, be written, but a substitute might be a signed and dated detailed note of a telephone reference given by a nominated third party to a competent (ie experienced in carrying out telephone reference checks) member of the organization's staff.
2. A completeness and accuracy check of the employee's curriculum vitae; this is usually carried out by means of written references supplied by previous employers or third-party organizations, and most employers will already have standard documents that are sent out to guide these third parties in replying. It is critical that the employer is methodical in ensuring that all facts are corroborated and that all forms are returned, duly completed, by previous employers. Where they are not returned within a defined time period (which should be short – perhaps 10 days at the outside), the organization should arrange to complete the form by means of a telephone interview with the previous employer.
3. Confirmation of claimed academic and professional qualifications, either by means of obtaining from the candidate copies of the certificates or other statement of qualification or through an independent CV checking service. These firms can, for a nominal sum, carry out detailed CV checks (including the checking of academic and other qualifications) that would satisfy the requirements of both point 2 above and this point 3.
4. There should be an independent identity check against a passport or similar document that shows a photograph of the employee.
5. A more detailed review of the individual's credit history and/or criminal record may be appropriate for those who will have access to more sensitive information. These checks are available from specialist providers.
6. Finally, and this is in addition to the ISO27002 list, the individual's entitlement to live and work in the country should be confirmed, by reference to appropriately endorsed travel or work documents.

Where a job, either on initial appointment or on promotion, involves access to information processing facilities, and particularly if it involves processing sensitive (financial or highly confidential) information, there should also be

a credit check. Where individuals have considerable authority in their position, this check should be repeated regularly, either quarterly or annually as appropriate.

Normal practice would be that, while a draft contract is agreed between the prospective employee and the organization, it is not signed and the employee does not start work until the checks have been completed. Depending on the outcome of a risk assessment, some organizations might choose to allow people to start work, particularly in roles that deal with only a low level of information, subject to satisfactory references; in these circumstances, it is necessary to set a time limit within which the reference checking will be complete. The contract of employment will usually not be signed by the organization until the reference checks are completed, and if they are unsatisfactory or not completed within the allocated time, the employee is dismissed. A similar process should be carried out for temporary or agency staff and contractors.

Where the staff are supplied by another organization (and this is often the case with IT staff, who are often directly employed by or contracted to the agency concerned), the contract with the third party should set out clearly its responsibility to carry out checks to a similar level. The contract also needs to set out what steps the agency has to take where answers to the screening process have been unsatisfactory or the process itself has not been completed. At the very least, these should include informing the employing organization, and in full, without delay, offering to replace any individual who has already started work, immediately and at no additional cost. The contracting organization should have adequate professional indemnity insurance, and this should be checked by obtaining and keeping on file a copy of the current insurance certificate.

While this may be relatively easy to implement for future hires, the organization has to decide what to do in respect of existing staff. It will not be sufficient simply to adopt the approach that because the staff are already there, there will be no problems. Undoubtedly, the correct approach to this situation is to ensure that the organization has records for existing staff of equivalent completeness to those required for new hires. It will be important that existing staff are made aware that this process is to be carried out and that it will be done openly and quickly.

Statistically, the likelihood is that every organization will discover that one or more members of its staff have incorrect or false CVs. Each of these instances will have to be tackled, and the organization will have to judge the extent to which the individual threatens its information security; the

organization's direct experience of the employee in the work environment may provide sufficient evidence to act on or to set aside the inaccuracy in the CV. If it is to be set aside, the employee should certainly be made aware that the inaccuracy was uncovered, and the reasons for its being set aside should be explained. This simple step can help the employee avoid such behaviours in the future.

New and/or inexperienced staff may, at certain times, have to be authorized to have access to sensitive systems. The company should identify what level of supervision will be required in such circumstances and ensure that it has in place a procedure for providing the appropriate level of supervision. The performance of all staff in respect of information security, particularly those who have access to sensitive information, should be reviewed on a regular basis (at least annually) and appropriate steps taken to ensure that the standards set by the organization are maintained. This review can be by means of one or more questions that are incorporated into an existing annual appraisal system.

At annual reviews, and on a day-to-day basis, line managers within the organization should be aware of unusual behaviour by members of staff that may be signs of stress, personal problems or financial challenges. Apart from the human benefits of helping employees deal with these challenges, such issues have been known to affect people's performance negatively (which may, of course, have implications for information security) and may also lead some individuals to commit crimes or fraud. Managers should be appropriately trained to spot and handle these situations within the restrictions of the relevant legislation.

Personnel vetting levels in respect of UK government information can vary according to the classification of material that the job holder will normally need to access. If you require advice on the application of clearance levels in this context, the appropriate department security officer will be able to advise you.

Terms and conditions of employment

Control 7.1.2 of ISO27002 says the organization should ensure that employees and contractors all agree and sign an employment contract that contains terms and conditions covering, *inter alia*, their and the organization's responsibilities for information security. These terms and conditions should include a confidentiality agreement, constructed in accordance with local

legal guidance, that covers information acquired prior to and during the employment and the effect of which should continue beyond the end of the employment.

This confidentiality agreement should be drafted by the organization's lawyers. It should form an integral part of the contract of employment, so that acceptance of terms of employment automatically includes acceptance of the confidentiality agreement.

There are circumstances in which someone who is working for the organization will not have signed an employment contract; he or she might, for instance, be working on a temporary or interim management basis, or even for short-term work experience. Anyone who has not signed a contract of employment should sign a confidentiality agreement of some description. This might form part of a contract for the provision of services or it might be a standalone confidentiality agreement. It should reflect the terms that are set out in the contract of employment, with any additional terms and sanctions that are recommended by the organization's lawyers in respect of these third-party relationships.

This confidentiality agreement is designed to cover situations in which a person is exposed to confidential information in the ordinary course of the employment or project, and it sets out the organization's requirements in these circumstances. It should cover legal responsibilities and rights in protection of copyright, intellectual property, data protection legislation, confidential and sensitive (particularly financially sensitive) information and any other relevant information issue. A different and specific non-disclosure agreement (NDA) should be signed by any organization to which confidential information will be disclosed pursuant to a business transaction.

The agreement should be signed and dated, and the original returned to the organization before the individual is granted any access to confidential information. The terms of specific agreements should be reviewed when an employee's circumstances change, particularly when he or she is due to leave the organization. It is often sensible to remind a departing employee (particularly someone who has had access to substantial amounts of confidential information in the course of the employment) of his or her obligations under the contract of employment and, in particular, of which obligations will survive termination of the employment. It is normal practice for compromise agreements to restate key confidentiality clauses.

Standard confidentiality agreements and NDAs should be reviewed after specific instances where loopholes in an existing agreement appear to have been found, and steps should be taken both to amend the document for the

future and, where the loophole is a significant one, to replace and re-sign existing confidentiality agreements and NDAs.

The contractual clauses should make clear that the employee has a responsibility for information security. This responsibility must be described. The simplest way to handle this is to attach the job description (and the separate statement of information security responsibilities, if this is the route that the organization has followed) to the contract of employment and for the contract of employment to refer explicitly to the responsibilities set out therein. As long as the information security clauses of the job description have been drafted in accordance with the guidance at the beginning of this chapter, and cover confidentiality, classification, responsibilities in regard to information received from third parties, responsibilities in respect of handling personal information, how the responsibilities are applied outside normal working hours and in any non-work (eg home) environment, and action to be taken in respect of anyone disregarding the organization's requirements, this requirement of the standard will have been met.

The guidance for control A.7.1.2 additionally recommends that an employee's or contractor's responsibilities in respect of compliance with relevant legislation should also be clearly stated. This is particularly important in terms of data protection legislation, copyright laws and computer misuse legislation. The contract should contain a clause (drafted by the organization's lawyers, and forming part of the contract of employment) that states that the individual will be personally responsible for ensuring that his or her activities in respect of information are not at any time or in any way in breach of these specific laws.

There is also the requirement to set clear rules for acceptable use of e-mail and the internet and, in the contract of employment, to set out very clearly the consequences for breaches of them. The rules do not need to be included in the contract, but the contract can refer explicitly to a section of the ISMS that contains them. E-mail usage rules are set out in detail in Chapter 20, as are acceptable internet use rules. Such policies must be consistently and firmly enforced; this sends a clear message to the organization that breaches will not be tolerated and helps build an environment of compliance.

During employment

Control 7.2.1 is a control requiring managers to ensure that everyone applies the organization's security policies and procedures; it is, in other

words, an extension of the requirements (see Chapter 3) that managers should be visibly committed to supporting the ISMS. ISO27002's guidance on this control includes ensuring that staff (employees and contractors) are: properly briefed on their roles and responsibilities before they are granted access to sensitive information or information systems (evidenced by their (electronic) signature on their access rights document (see Chapter 12); motivated to fulfil their roles and conform to the policies (evidenced through the internal audit process); aware of information security threats, risks and vulnerabilities; and will maintain their competence.

Clauses 7.2 and 7.3 of the standard and control A.7.2 (information security awareness and training) require the organization to ensure that its employees and contractors are aware of information security threats as well as their responsibilities and liabilities, and that it has appropriately competent personnel. The objective of this clause is simply to ensure that all users of the organization's information assets, or those who are assigned responsibilities in the ISMS, are aware of information security threats and are competent and adequately equipped to perform the requested tasks and to support the organization's information security policy in their work.

Control A.7.2.2 deals with information security awareness, education and training, and follows on from the previous control. All employees of the organization (including contractors) must receive appropriate awareness training and other training, as well as regular updates and communications.

Traditional training, which relies on someone delivering subject matter from the front of the classroom, is not a particularly effective method of ensuring that all of a large number of employees acquire the information, skills or knowledge that are needed. It is certainly not a method that reliably demonstrates that this requirement of the standard has been met. The best way of delivering information security staff awareness training is via e-learning that is run on a recognized learning management system (LMS) or in a cloud-based environment, supported by a range of wall posters and computer screen reminders and related material.

Staff awareness e-learning can be delivered directly on to the desktop workstation of the targeted employee. It can be delivered in a way that improves uptake and retention as compared with traditional classroom training. It can be delivered through the web or rolled out quickly using the corporate network. It can be delivered to a consistent standard across an entire organization, and geography is no real barrier. The learning can be accessed by employees at a time to suit them, and because trainees are not required to go away on a training course, productivity is not affected by

e-learning. In fact, e-learning can be less expensive as a method of rolling out training than the traditional classroom approach, both because of these productivity benefits and because none of the usual costs of attending courses (whether internal or external) need to be incurred. There are a number of suppliers of e-learning products; one that can supply an appropriate suite of ISO27001 products virtually off the shelf is likely to be less expensive as an option than an organization that makes a bespoke package specifically for its client. Information about information security e-learning and other awareness products is available from www.itgovernance.co.uk/information-security-awareness (archived at https://perma.cc/5XRU-CYVU).

Web-based e-learning and any recognized LMS will both support network- based e-learning and provide a real audit trail that produces records of who has accepted specific policies, who has completed which e-learning modules and when they were done. The LMS can also run tests that can demonstrate the level of competence that the trainee has acquired in the subject matter. Administration of these systems can be done cost-effectively online.

E-learning is particularly cost-effective for training large numbers of staff. Small numbers of staff, particularly those who need detailed and extensive training, often involving feedback, questions and answers, coaching, etc, are better dealt with in the classroom. The areas of information security and the ISMS that are best dealt with through e-learning and that begin as part of the induction process are as follows:

- all-staff briefing – ISMS awareness, known threats and the importance of information security and the ISMS, including general controls;
- asset classification and control;
- reporting events and responding to security incidents and malfunctions;
- e-mail and web access awareness and rules;
- user access control and responsibilities;
- mobile computing and teleworking;
- legal compliance awareness and related issues;
- business continuity awareness and procedures.

Any staff involved in handling payment card data, and working within a cardholder data environment as defined by the PCI DSS, will also need specific training on their responsibilities in regard to that data.

There are also a number of staff who will require other user-specific training. These include the staff identified at the beginning of this chapter as needing specific statements in their job descriptions and contracts of employment about their information security responsibilities. These include:

- the chief information officer and/or chief information security officer;
- the information security adviser;
- members of the information security management forum;
- IT managers;
- network managers;
- IT and helpdesk support staff;
- webmasters;
- premises security staff;
- HR, recruitment and training staff;
- general managers;
- finance staff;
- the company secretary and legal staff;
- internal management or system auditors;
- business continuity and emergency response teams.

These staff should be exposed to the same all-staff training as discussed above. In addition, user-specific training will be required. The necessary training is best identified though an individual training needs analysis (TNA). The organization is likely to have a TNA process in place, and this should be applied to the security training issues. Those organizations that do not already have a TNA process in place have the choice between designing and implementing a process that will cover all of its training issues going forward, and implementing one that simply works for the information security training needs. Information security training is better tackled, on an ongoing basis, as part of a structured organizational approach to employee training. However, in situations where it is necessary to get security-specific training started, it may be simplest to apply a TNA process to deal specifically with information security training.

Any handbook on corporate training, or a training professional, could provide appropriate support on a step that is fundamental to well-designed

training delivery. The principle underlying a TNA is that once the knowledge, skills and competency requirements of a particular role have been clearly established, and documented in the job description, the role holder's own knowledge, skills and competence can be compared to the requirement and a gap analysis, or TNA, completed. The next step is to map out an individual learning path that will meet the requirements of the TNA and close the knowledge, skills and competence gap. This individual learning path will contain a mix of self-learning, instructor-led training and experience. It should identify clearly where the training is to come from and should set out the dates by when specific steps are to be taken, identified skills or competencies acquired and proof of acquisition generated. There is far more to a TNA than this, so do make use of a training professional to do the job properly.

While most organizations will have a TNA process in place for groups of staff, which identifies the gap between the individual's skills and those of the generic role, there are individuals who, for information security purposes, must have very specific knowledge, skills and competencies that are in addition to those needed by a group of employees of which they may be a part. Clause 7.2.2 expects that there will be an individual TNA, based on an individual or additional assessment of the knowledge, skills and competence required for each of these roles, for each of the people in one of the individual or specialist roles identified above. Where this is being put together for a new employee, the offer letter might make permanent employment conditional on achieving certain stages within certain time-frames.

Clause 7.2 of the standard requires the organization to maintain records of competence and this requirement is satisfied by following the recommendations of this chapter and attaching records of education, training, skills, experience and qualifications to the individual's personnel file. More importantly, the effectiveness of the training must be evaluated, and this requires the specific objectives for each piece of training, and the criteria for measuring its effectiveness, to be identified and agreed in advance. This is in line with best practice for effective staff training.

Training should clearly be delivered by competent trainers. In Chapter 4, there is an initial discussion on appropriate training for specialist information security advisers and the specialist training resources on the IBITGQ and IT Governance websites. This site should enable appropriate trainers for the various IT specialists to be identified.

Those IT staff charged with systems administration should be appropriately trained, by either the software supplier or by an approved training

vendor, as system administrators for the software for which they are the nominated administrators. Evidence of this training should be retained on each individual's personnel file. Those responsible for firewall, antivirus, encryption and any other security software should have appropriate training certificates and should be required to keep their skills and knowledge current by attending regular refresher and update courses. These should be booked into the individual's training calendar in advance and there should be evidence that they were attended. Certainly, in any Microsoft environment there should always be a systems administrator who has a Microsoft certificate with the security extension, such as the MCSE with security.

Webmasters, in particular, need to be thoroughly trained and have their skills regularly updated. Their training needs to cover the security aspects of all the hardware and software for which they are responsible; in particular, they need to be capable of ensuring that the web servers are correctly configured and fully secured. It is essential that all high-risk systems are 'hardened' to at least the minimum standards identified by Microsoft on its technet website. Webmasters must be able to handle this.

Information security staff, company secretaries and legal staff and HR or personnel staff will also need specific legal training. There are a number of specific legal issues to do with information security (all discussed in Chapter 27), and the organization needs to know how to handle them, using standard template documents wherever possible. It does not need to employ an in-house lawyer, as this can be unnecessarily expensive; external expertise can be brought in where and when necessary to deal with specific legal issues.

Staff dealing with voice systems and network hardware and software will all need specific, supplier-certified administration and security training that covers these products. The organization will need access to regular updates on information security issues relating to these products.

There is a discussion in Chapter 27 about training for internal auditors.

There are two effective ways (particularly for a multi-site organization) to make information security related material available to everyone in the organization. The first is to use a document management system that pushes information out to users across the network, usually in conjunction with ensuring that they are aware of policy and procedural issues. The second is to put it on a shared drive, an intranet or SharePoint. Either the organization already has an intranet, or SharePoint, in which case it simply needs to create an information security sector on it (or within the quality management sector), or it could consider setting up an intranet or SharePoint. This

does not need to be an expensive step and is undoubtedly the best way of dealing with information sharing. The organization's existing webmaster or IT manager may have the skills necessary to set up SharePoint or it may be necessary to arrange appropriate training. Deployment of SharePoint does bring additional challenges of its own and, if this is the organization's preferred course, it would be sensible to investigate how to deploy SharePoint server governance. Of course, it will also be necessary to ensure that appropriate guidance on procedures is available to any affected staff in case of a system crash. This could mean that paper versions of the procedures should be available or, alternatively, a notebook computer with an up-to-date set of procedures that is part of the emergency response equipment.

The benefits of using SharePoint are that it can be the single repository of controlled documents; the information security manual and procedures can all be stored there and staff can be trained to access the relevant SharePoint site for anything to do with information security. It is easy to keep the controlled documentation up to date and to ensure that document control is effective. It is then easy to alert all relevant members of staff about changes to procedure simply by sending out an internal e-mail, with an appropriate link, that tells them which sections of the ISMS have been changed. Twitter might be another alternative. SharePoint can also have a section that carries information about information security developments and issues of which staff need to be aware. Someone within the organization needs to have the responsibility for keeping the site up to date, and this person obviously will need to be appropriately trained. The people who might have this role include the information security adviser, the quality manager, the marketing manager (if the marketing department has responsibility for internal communications) or the webmaster.

Disciplinary process

Control 7.2.3 of ISO27002 says the organization should deal with employee (and contractor) violations of its information security policy and procedures through a formal disciplinary process. Obviously, the organization should use its existing disciplinary process, and should be clear about this in employee contracts (as discussed earlier in this chapter) and in the ISMS itself.

Clearly, no disciplinary process can start until the existence of a breach has been verified (and control 16.1.7 deals with evidence collection), and formal commencement criteria may need to be documented that are legal in

the local jurisdiction. The organization should ensure that those who are carrying out a disciplinary hearing in respect of a reported violation of an information security procedure are given the professional and technical support that they might need in order to deal fairly with the person and the issue. This might require the organization's information security adviser to be involved in the process. On no account should inexperienced, uninformed managers attempt to deal with information security matters that are beyond their knowledge or experience, as this would be unfair to the employee concerned and potentially dangerous for the organization if the full implications of an incident are not understood quickly enough. It could also, depending on the outcome of a disciplinary hearing conducted by an inexperienced manager, potentially expose the organization to time-consuming and expensive industrial tribunal actions or trade union challenges for unfair treatment of an employee.

Termination or change of employment

The control area (A.7.3) dealing with termination or change of employment has a single control (A.7.3.1) that should work alongside A.8.1.4 (Return of assets) and A.9.2.6 (Removal or adjustment of access rights). In many organizations, experience suggests that administration of employment termination is, in information security terms, often sloppy. As a result. organizations are creating new vulnerabilities that needed to be assessed. The control objectives here are to ensure that termination of employment (or a change in job role) is carried out in an ordered, controlled and systematic manner, with the return of all equipment and removal of all access rights.

Control 7.3.1 deals with termination responsibilities and simply says the organization should document clearly who is responsible for performing terminations and what these responsibilities are. These responsibilities should clearly include dealing with the ongoing clauses in the contract of employment. Usually, the HR department will be responsible for ensuring that all the termination aspects of an employment contract have been dealt with (usually in conjunction with the ex-employee's line manager), and these may be standard aspects of a termination interview, which is carried out in a standard way, using a standard checklist.

The termination of contractors needs also to be dealt with. The organization simply needs to determine how it will achieve, with these personnel, the

same clarity as it seeks with ex-employees and who (agency, third-party organization) will be responsible for performing the task.

Control 8.1.4 requires all employees, third parties and contractors to return all organizational assets upon termination. As well as financial assets (eg credit cards and purchase orders) and HR or fixed assets (eg company cars), these assets fall into four categories: software, hardware, information and knowledge. Subject to local employment law, the contract of employment should have a clause that allows the employer to withhold any outstanding payments of any description until all organizational assets are proven to have been returned and, after a suitable interval, to deduct from any such outstanding amounts the cost of replacing assets that have not been returned. Of course, this will tend to push the majority of resignations to the day immediately after monthly or other substantial payments have cleared the employee's bank account, but such is life.

The first two asset types are best dealt with procedurally through a centralized recording and authorization process; there should be a record for each employee (maintained by the HR or IT department) that lists all laptops, smartphones and other hardware issued to employees. This list could be linked to the asset inventory discussed in Chapter 9, and the nominated owner or custodian should clearly be the person to whom the asset is issued. There should be an acceptable use document for each asset, describing what has been provided (and laptops should have a standard, documented 'kit'; while laptops are often returned, the accessories are often missed), setting out clearly the organization's expectations for the proper use of the asset and including (eg for mobile telephones) any expectations about how costs are to be split between employee and organization.

Information – classified documents, whether electronic or paper – should also all be returned. In fact, it is difficult to identify what documentation any individual has removed during the course of employment (unless they were limited-circulation numbered documents), and this control is, in practical terms, best met through the termination interview. One standing item on the schedule for this interview should be a question as to whether or not the employee has any classified information and, if none, a reminder that any such documents must be returned.

Knowledge – the skills and competence that a terminated employee may have – should be retained in the organization. This is, in real terms, not easy to achieve. In the case of people who have critical knowledge, there should be a risk assessment prior to starting any termination action, to identify any

knowledge that must be retained and to plan methods of retaining it. Unless this step is taken, one can assume that the knowledge – particularly if it is held by someone who is being unwillingly terminated – will leave the company with the employee. It is not unknown for organizations to delay commencing termination procedures with employees until the employees have successfully transferred their knowledge.

Control 9.2.6, removal of access rights, is critical, as access rights may enable a disgruntled ex-employee to compromise a system; this section should be read in conjunction with Chapter 11. The organization needs a clear documented procedure to ensure that upon termination (and sometimes – subject to risk assessment and local legislation – before termination), an employee's (or contractor's) access rights are also terminated. Similarly, any change in employment should also lead to a review and adjustment of existing access rights. These access rights include passwords, tokens and other authentication rights, e-mail and internet user accounts and user names, electronic files, etc and should be extended to include any identification cards, including business cards and headed notepaper. It may be necessary for ex-employee e-mail accounts to continue in use for a period after termination, and this should be covered by a standard policy that sets out how the e-mail auto-responder should be set up, who should have ownership of the account and how any incoming e-mails should be treated.

9

Asset management

Control objective A.8 of the standard deals with asset management, including classification, acceptable use and media handling. The overall objective here is for the organization to achieve and maintain appropriate protection of organizational assets.

Asset owners

Control 8.1.2 of ISO27002 says that all information assets should have a nominated owner ('an individual or entity that has approved management responsibility for… the assets') and should be accounted for. Clearly, the 'owner' is the person, or function, that has responsibility for the whole lifecycle of the asset; the 'owner' has no property rights to the asset. This control requires the asset owners to ensure assets are inventoried and this inventory should be used during the risk assessment, as discussed in Chapter 6. The nominated owner of each of these assets should be a member of staff whose seniority is appropriate for the value of the asset that he or she 'owns'. This person's responsibility for the asset should be tied to his or her role, and set out and described in a letter, or memorandum, to him or her. The fact that the asset is owned by a role means that documentation does not have to be reissued every time the name of the person holding the role changes.

The nominated asset owner should sign the memorandum to acknowledge agreement to it, and this signed original should be placed on his or her personnel file. Either a copy should be retained along with the asset schedule or the schedule should name the role that owns the asset and refer to the personnel file for it. Alternatively, this information could be contained in a signed job description or the contract of employment itself.

There should be a description of the asset(s) for which each person is responsible and its (or their) location(s). It should describe the security controls (including the security classification and access restrictions) that are required for the asset and set out the owner's or custodian's responsibility for maintaining (and periodically reviewing) them. The owner may be allowed to delegate routine tasks in relation to their assets but the responsibility for implementing or maintaining controls across the whole lifecycle of the asset remains with the owner. Accountability, in other words, should rest squarely and clearly with the nominated owner. Custodians are those to whom an asset owner has passed custody of an asset; the custodian must adhere to requirements defined by the owner.

The asset owner can also be a specific department or 'entity' within the organization, and in some circumstances (where there may be high staff turnover, such as in a call centre) it may be appropriate for the asset owner to be the department or manager responsible for the area. The key consideration, when assigning ownership to a department, is to ensure that an individual in a specific role will exercise that accountability – otherwise information security requirements are unlikely to be actioned.

Inventory

Control 8.1.1 specifically says the organization should identify all assets that are important to their information lifecycle and to draw up and maintain an inventory of them. Of course, generally accepted accounting practice and legislation already require companies to maintain registers of all fixed assets within the organization. However, this requirement does not in practice automatically extend to public-sector organizations. Furthermore, the assets that are covered by the fixed asset register do not normally include all the information assets of the company, particularly not the intangible information assets. Moreover, the accounting fixed asset register reduces the value of assets over time, whereas many information assets either maintain value, or see their value increase over time.

The information assets of the organization should be identified during the risk assessment process (see Chapter 6), and the resulting schedule should be checked against the fixed asset register to ensure that no assets have been missed. The inventory should have a nominated owner, and the procedures for maintaining it and, in particular, for accessing it in a disaster recovery situation should be clearly documented. The fixed asset register can

also provide historic information about the cost of the asset, and this information may be useful in helping identify the relative importance and value of the assets. ISO27005 provides more detailed guidance on how to value assets on the basis of the impact that compromises of their availability, confidentiality and integrity may have on the organization.

Risk assessment tools, such as vsRisk™, are built around an asset database that can maintain the asset inventory for the ISMS; in this case, the lead risk assessor is likely to be the owner of the inventory.

The asset inventory should identify each asset, including all the software, and describe it or provide such other identification that the asset can be physically identified (wherever possible, it makes sense to reuse whatever fixed asset number has already been allocated) and full details (including maker, model, generic type, serial number, date of acquisition and any other numbers) included in the inventory. Its current location should be stated. Any other information necessary for disaster recovery (including format, back-up details and licence information) should be listed. The nominated owner (and, if this is different, the name of the operator) of the item should be shown on the schedule, as should its security classification (see below). The inventory should be updated for disposals (when and to whom). Physical inventory checks should be carried out at least annually, by someone other than the nominated owner of the asset, to confirm the accuracy of the register. The types of assets that might need to be inventoried include the following:

- Information assets: data in any format. Files and copies of plans, system documentation, original user manuals, original training material, operational or other support procedures, continuity plans and other fall-back arrangements, archived information, personal data, financial and accounting information.
- Software assets: application software, operating system software, development tools and utilities, e-learning assets, network tools and utilities.
- Physical assets: sites, computer equipment (including workstations, notebooks, smartphones, monitors, modems, scanning machines, printers), communications equipment (routers, mobile and smartphones, PABXs, fax machines, answering machines, voice conferencing units, etc), magnetic media (CD ROMs, tapes, disks, USB sticks, external hard drives), other technical equipment (power supplies, air-conditioning units), furniture, heaters, lights and other equipment.
- Services: general utilities, eg gas, electricity and water.

- People: their qualifications, skills and experience – the knowledge and skill capital of the organization. This is a particularly complex process for which external consultancy help might be sought.
- Intangible assets such as reputation and brand. There are established methods of valuing intangible assets and a range of issues to be taken into account, including whether or not the intangible assets should be listed on the balance sheet. Certainly, reputation is one of the most important intangible assets, and boards should make a constructive effort to establish its value. Including reputation as an asset does not stop you including reputation damage as part of the impact estimate in the risk assessment when considering the consequence of individual assets being compromised.

Usually, whoever is responsible for the facilities management in the organization will be the nominated owner of the services (see 'Services' in the list above) and a number of the physical assets. The IT manager and individual system administrators will usually be responsible for the other physical assets and the software assets, although a number of individual users ('custodians', as described earlier) are likely to be responsible for the notebook or mobile device or any other, similar, item that they have been assigned.

It is much more difficult to determine the owners of the intangible information assets. It is important to get this right because the owner will have specific responsibilities. In terms of new documents, the organization could simply adopt the policy that the originator of an information asset will be defined as its owner. This is meaningful in terms of information assets that will have, generally, a specific and limited use, which is driven by the originator. This would cover, for instance, business plans, forecasts, client letters and project plans.

There are other information assets, however, the use of which through the organization will be widespread and has originated as the result of a strategic or group decision. Examples might include customer relationship management (CRM) systems and their client data, workflow systems and the information they contain, accounting systems and financial information. (Increasingly, these systems might be outsourced, so the owner of the asset will also be the owner of the relevant third-party relationship.) The default approach, in many organizations, is for the IT department to be the owner of these assets. This is not always the most sensible approach, as it divorces the system from those most committed to its effective use. The most practical approach to these assets is for the organization, at the time that it decides

to deploy the asset, to decide who will be the owner and to write this into the person's job description. Usually, the owner should be the person who uses it most, or has most control over it: the financial controller might be the nominated owner of the accounting system and the sales manager might be the nominated owner of the CRM data.

It may be practical for this defined ownership to be time-bound. Sensitive incoming mail from a client may first, for instance, belong to the corporate services function until the relevant sales or customer relationship manager is identified and the ownership is then passed to him or her. It would also not be unreasonable to state that, once archived, the ownership of data passes to the facilities or library function, and that the value of the archived information will start to diminish from this point. Clearly, the impact of a breach decreases at the same time and this should be reflected in the risk assessment.

The process of identifying owners for information assets needs to be sensible. The organization is likely to have many items of information that have little or no practical value; there is little point in nominating owners for this information and going through the steps covering classification and control, for it will be time-consuming and the exercise will fail any cost–benefit test. It would be better for the organization to implement a procedure that defines the threshold above which information will be considered an asset and above which, therefore, it will be subject to the controls specified in this section of the standard. Some organizations opt for a catch-all default level for such information.

The way to do this is through the information classification procedure, which is discussed below. Information with a specific low-level classification, assigned by its owner, may be defined as not being an asset worth protecting, and information with all other classifications may be defined as assets and worth protecting. For instance, a file of press cuttings might be classified such that it is clear that it is not an asset worth protecting; statutory accounts, once filed at Companies House, become public domain information, which there is no point in protecting from a confidentiality angle (although the integrity and availability of these data could still be of concern).

Acceptable use of assets

Control 8.1.3 of ISO27002 says organizations should document and implement rules for the acceptable use of information assets, systems and services.

These rules should apply to employees just as much as to contractors and third parties, and the particularly important areas for which acceptable use policies should be drawn up include e-mail and internet usage, mobile devices (telephones, mobile devices and laptops) and usage of information systems beyond the organization's fixed perimeter. Chapter 12 deals with this issue in detail and provides sufficient guidance to enable the organization to draw up and implement adequate acceptable use policies.

Control A.8.1.4 is covered in Chapter 8.

Information classification

Control 8.2 provides for the organization to have a procedure for classifying information that will ensure that its information assets receive an appropriate level of protection. Control objective A.8.2.1 is that information should be classified in terms of legal requirements, value, criticality and sensitivity, and guidance on how to achieve this is in clause 8.2.1 of ISO27002. Classifications and protective marking controls should be suited to business needs (including legality, value, sensitivity and criticality) both to restrict and to share information, and to the business impacts associated with those needs. It is important to note that sharing is as important an objective of this section as is restricting; it is possible to draw up a set of guidelines that are too restrictive for the business and that are therefore regularly breached. This is not a useful outcome. Organizations (particularly in today's environment) depend on sharing information; it is essential that information is classified in such a way that this can be done consistently and appropriately. Whatever classification scheme is adopted by the organization should be extended across the whole organization, and should cover the level at which users can access data in the system (read only, write and delete).

Information classification is a key concept in the structuring and development of an effective ISMS. The classification given to a particular information asset can determine how it is to be protected, who is to have access to it, what networks it can run on, etc. 'Confidentiality' is, after all, one of the three key objectives of an ISMS and includes non-disclosure to unauthorized processes.

The benefits of adopting a consistent procedure are clear. The organization will:

- reduce the risk of damage to its reputation, profitability or interests due to loss of sensitive information;

- reduce the risk of embarrassment or loss of business arising from loss of another organization's sensitive information;
- increase confidence in trading and funding partnerships and in the outsourcing of sensitive activities;
- simplify the exchange of sensitive information with third parties, while ensuring that risks are appropriately managed.

Classified information is marked so that both originator and recipient know how to apply appropriate security to it. The classification is based on the likely impact on the organization if the information is leaked or disclosed to the wrong third-party organizations or people. It does not matter what system the organization adopts, provided it is clear, clearly documented and clearly understood by all staff and everyone who uses it.

The simplest approach is usually one that has only three levels of classification. The first level might be to identify that information which is so confidential that it has to be restricted to the board and specific professional advisers. Information that falls into this category might be marked 'Confidential', with the names of the people to whom it is restricted identified on the document. Some organizations also number documents that have this level of classification, so that each person who is sent a copy receives a numbered copy. Usually, all pages of such a document would show the classification in capital letters at least 5 millimetres high and, if it exists, the individual number. This information should be included in the document header, which should be set to appear on all pages of the document. Examples of confidential information might include information about potential acquisitions or corporate strategy, or about key organizational personnel, such as the CEO. The amount of information that falls into this category should be carefully limited; the cost and operational inconvenience of protecting it properly is such that the category needs to be restricted to information the release of which could significantly damage the organization.

A second level of classification might cover documents that are to be available only to senior or other specified levels of management within the organization. These might be marked 'Restricted'; the related procedure should specify a level of employee above which anyone can access the document. Examples might include draft statutory accounts, which might be available to everyone in senior management, or implementation plans for corporate restructuring, which senior managers need to work through prior to their being rolled out. These documents are usually not numbered, but the decision to release them (which is, by definition, a decision to release

them to everyone in the organization who is entitled to receive information of this level) should not be taken lightly.

The final level of classification might be, simply, 'Private', and this should cover everything that has value but that does not need to fall within either of the other categories. Everyone employed by the organization should be entitled to access information with this classification. At the same time as adopting such a system, the organization should make clear how it will treat any internally originated documents that carry classifications (eg 'Private and confidential', or 'Restricted – commercial in confidence', or any other variations on the theme) other than those described in the procedure. Such incorrectly classified documents could be either automatically destroyed, or automatically reclassified, or automatically treated as having no classification at all; the policy decision should reflect the risk and cultural environment within which the new classification system is being adopted. The organization also needs to consider how it will appropriately reclassify third-party-sensitive documents that it receives, which may have an incompatible classification, and that it will be responsible for protecting.

It will be important, in deciding which employees will have access to which levels of information, to resolve what is to be done in respect of those employees who have to support senior managers but who themselves might fall into a lower classification in terms of information security. An implication of this might be the rather farcical one of people such as personal assistants and secretaries working on or distributing documents or supporting meetings whose content they have to try not to be aware of. Far better, frankly, to allow these people the same level of access to confidential documents as their managers and to take all the necessary steps to ensure that only appropriate people are recruited into these roles.

The 'effects of aggregation' should be considered; it is possible for a series of non-confidential items to become confidential when they are aggregated. For example, individual pages of a set of accounts might not, in themselves, be confidential (because they carry incomplete information) but together they might be valuable and confidential. The best way to deal with these types of issues is to apply from the outset the aggregate-level classification to all the component parts of the information asset.

Unified classification markings

Wikipedia has a very useful, reasonably thorough page on classification systems, which deals for instance with various national classification systems

as well as those of the UN and NATO. An older, no longer common framework provides a clear, independent, coherent classification system which is still useful for describing the elements of an effective system.

The unified classification markings had three levels of information classification. An advantage of a universal system is that the markings are reasonably widely known, so they can be added to an internal classification when a document is passed outside the organization in order to help the recipient apply appropriate protection.

SEC1 is defined as information the unauthorized disclosure of which, particularly outside the organization, would be inappropriate and inconvenient. This is routine information that an organization simply wishes to keep private. This classification may not need to be marked on information; it refers to the greater part of the organization's information. This information is usually commercially valuable, and while SEC1 may be an appropriate classification in a low-risk business environment, there will be other business environments in which this may be too low a classification.

SEC2 is defined as information the unauthorized disclosure of which (even within the organization) would cause significant harm to the interests of the organization. This would normally inflict harm by virtue of financial loss, loss of profitability or opportunity, embarrassment or loss of reputation. Such information might include:

- negotiating positions;
- marketing information;
- competitor assessments;
- personnel information;
- customer information;
- restricted government material.

SEC3 information is defined as information the unauthorized disclosure of which (even within the organization) would cause serious damage to the interests of the organization. It would normally inflict harm by causing serious financial loss, severe loss of profitability or of opportunity, grave embarrassment or loss of reputation. This information might include:

- details of major acquisitions, mergers or divestments;
- high-level business or competition strategy;
- very sensitive partner, competitor or vendor assessments;
- high-level business plans and scenarios;

- secret patent information;
- highly confidential government material.

Information that is required, under the policy adopted by the organization, to be classified must be appropriately marked. This marking must appear wherever the information appears, be it on paper, cassette, disk, flipchart, film, microfiche, etc. Where information carries no classification, it is regarded as having no value.

When organizations are going to exchange information, they should ensure that each understands the other's classification system. The ISO27001 organization will want to ensure that it has in place a methodology for applying to information received from a third party a classification that is in accordance with both the originator's and its own system. No organization should under-protect another organization's information; in circumstances where the receiving organization would classify particular information at a lower equivalent level than that applied by the originator, the recipient should apply a higher classification than it would to an internal document. Those companies that apply an SEC1 level of classification should make it clear to third-party organizations that this type of information is freely available within the organization. Those organizations that do not even apply an SEC1 classification should make it clear to third parties that this sort of information is not handled securely.

Government classification markings

National governments have developed their own security classification schemes. The nature of these national schemes is affected by issues such as the existence or otherwise of freedom of information legislation and the nature of date protection and privacy regulation. Wikipedia (https://en.wikipedia.org/wiki/Classified_information (archived at https://perma.cc/4ZVV-UWKW)) describes government classification schemes in a number of countries. The EU and NATO have specific information classification schemes, and the G8 developed its Traffic Light protocol, for documents that might be shared between member countries.

In the United Kingdom, the Security Policy Framework (SPF) sets out the information security requirements for the UK public sector.

This system now has three levels of classification or protective marking. In descending order of secrecy, these are: Top Secret, Secret, and Official;

documents without a classification are marked 'Unclassified' or 'Not Protectively Marked' to indicate that protective marking is not required. Mandatory requirement no 19, in the SPF, describes how these markings should be applied:

a Access is granted on a genuine 'need to know' basis.

b Assets must be clearly and conspicuously marked. Where this is not practical (for example the asset is a building, computer) staff must still have the appropriate personnel security control and be made aware of the protection and controls required.

c Only the originator or designated owner can protectively mark an asset. Any change to the protective marking requires the originator or designated owner's permission. If they cannot be traced, a marking may be changed, but only by consensus with other key recipients.

d Assets sent overseas (including to UK posts) must be protected as indicated by the originator's marking and in accordance with any international agreement. Particular care must be taken to protect assets from foreign Freedom of Information legislation by use of national prefixes and caveats or special handling instructions.

e No official record, held on any media, can be destroyed unless it has been formally reviewed for historical interest under the provisions of the Public Records Act.

f A file, or group of protectively marked documents or assets, must carry the protective marking of the highest marked document or asset contained within it (eg a file containing CONFIDENTIAL and RESTRICTED material must be marked CONFIDENTIAL).

The US government has a classification scheme that uses only three levels: Confidential, Secret, and Top Secret.

Information lifecycle

Information does not always have to remain classified at the same level at all times. Statutory accounts, for instance, are confidential until they have been signed and filed at Companies House. The classification applied to them should be appropriately reviewed and the organization's procedure should

require originators to review the classification of key documents on a regular basis. Some information is sensitive only for a specified period. Where this is the case, the information should show the date beyond which it will no longer be sensitive. This is common practice with, for instance, press releases, which are usually sent out with a legend along the lines of 'embargoed until 0000 hours on x day'.

Information labelling and handling

Control A.8.2.2 and A.8.2.3 of the standard says the organization should implement a set of procedures for information labelling and handling that reflects the information classification scheme (as above) that it has adopted. As ISO27002 says, these procedures need to cover all formats of information asset, both physical and electronic. There should be procedures for the following types of information processing activity:

- acquisition of information;
- copying (electronically, by hand and through reading and memorizing);
- storage, both electronic and in hard copy;
- transmission by fax, post, e-mail and wireless synchronization;
- transmission by spoken word, including mobile phone, voicemail and answering machines;
- chain of custody and logging of security events – particularly important when dealing with computer-related crime;
- destruction when no longer required.

The types of procedure that could be adopted for each of the unified classified markings are set out below. The procedures should be adapted as necessary and incorporated into a simple organizational classification procedure within the ISMS, and everyone responsible for handling the information should be trained in how to apply them. Specific consideration needs to be given to the labelling of electronic assets, and the input of the IT team will be required to define an effective means for applying the chosen classification to electronic assets and media in a way that is rigorous and reliable. Alternatively, digital classification software can be purchased and deployed.

SEC1

- Information that has no marking can also be treated as information that has an SEC1 classification. It can be released to anyone outside the organization at the discretion of the information owner. It should be handled and processed within a secure perimeter, and at the end of the day should be cleared away. Removable material should be put away when it is not in use and electronic equipment that is not being used should be switched off.
- External mail should be sealed.
- E-mail should only be sent over networks that are considered to be secure to at least this (SEC1) level and should not contain attachments that are classified at a higher level.
- Destruction of papers should be through an approved office waste disposal company that has a contract that meets the organization's standards terms and conditions.

The final items that need to be considered in terms of information classification are faxes and e-mail. Faxes are still used and e-mail is ubiquitous; both are so unreliable that secure documents could easily be delivered to the wrong person. A part of dealing with this risk is the use of standard disclaimers on both faxes and e-mails, although these do nothing to control the likelihood of such a threat and are of little practical use in addressing the impact of such an incident. Policies on the use of faxes, enforced in the appropriate fashion, need to complement the disclaimer as a control. The fax disclaimer should be clearly printed on the fax cover sheet and it should be a procedural requirement that all faxes use the standard cover sheet. For preference, the disclaimer should be included on the desktop system in the template for a standard fax cover sheet.

On e-mails, the disclaimer should be built into the standard organizational signature that is attached to all e-mails. The network administrator can set this up so that the organization's chosen disclaimer is included as a standard default in all e-mails, irrespective of the wishes of the e-mail originator, but so that the individual's chosen signature can also appear on the e-mail. A possible e-mail disclaimer is set out below, but is likely to need the additional statement (that any opinions expressed are those of the author and do not reflect in any way those of the organization) that is discussed in Chapter 20. Information about the originating organization may also be

required. Any version of this disclaimer actually deployed by any organization must first be approved by its own legal advisers to ensure compliance with current legislation.

LEGAL DISCLAIMER

Here is an example.

> This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message that arise as a result of e-mail transmission. If verification is required, please request a hard-copy version. This message is provided for informational purposes only.

Additional statements should be added to this to protect the organization against libel actions, and these are discussed in Chapter 20.

SEC2

SEC2 material needs more stringent controls:

- All pages of, and physical media containing, SEC2 material should be clearly marked as such. Access to it should be limited to those with a need to know and it should be stored in a way that makes it unlikely that it will be compromised by accident or through opportunism and that should deter deliberate compromise of it.
- Destruction should be done in a way that makes its reconstitution difficult.
- Personnel who will handle this classification of material need to have had appropriate security checks carried out.
- It should be handled within a secure perimeter, and steps should be taken to ensure that material cannot be observed by unauthorized people.
- IT systems handling this level of information should themselves be located within a managed security perimeter; effective access controls

should be in force and appropriate monitoring procedures that deter unauthorized access should also be in place.

- This material should only be disclosed on a need-to-know basis, and steps should be taken to ensure that the recipient is aware of the sensitivity level and the implications for its protection.
- SEC2 information should not be verbally disclosed in a public place where it could be overheard by others.
- Letters should be sealed and sent in such a way that the sensitivity level of the information cannot be deduced from the outside of the letter; such letters might be marked 'To be opened by addressee only'. If sent externally, it should probably be within a cover envelope that does not reveal the security level of its contents.
- Faxes should only be sent once it has been confirmed that the receiving station is the correct one, and that it is ready to receive, secured to an SEC2 level and attended by a trusted person. The fax should only be sent by an appropriately trusted person.
- Steps should be taken to ensure that conversations are not overheard, and telephones in public, or hotels, or obviously insecure locations (overseas, or competitors' offices) should not be used as they are easy to listen in on or overhear.
- Any messages sent via the internet should only be sent once they have been appropriately secured by means of an approved encryption method. Internet connections should only be made via an approved and secure firewall. Internally, the information should only be shared on an electronic system that is secured to at least an SEC2 level.
- SEC2 material should be destroyed by an approved person or organization that will shred or otherwise effectively destroy it. Removable media should be encrypted and overwritten before reuse; media that cannot be overwritten should be destroyed by an approved company and not reused. Back-up copies should be encrypted and all back-up copies should also be destroyed at the point that the original is destroyed.
- SEC2 documents and devices carrying information of this level of sensitivity should be supervised at all times, and when not in use should be safely locked away, including in secure facilities in hotels when travelling. Notebooks and mobile devices should have boot-level encryption to a recognized international standard.

SEC3

SEC3 material needs much more stringent safeguards. It requires the SEC2 controls, plus additional ones, as described below:

- SEC3 material should be marked as such. Access should, clearly, be limited to those authorized to see and use the information. It should not be disclosed unless there is a good business, contractual or legislative need to do so. Assurance (by means of a signed form) should be sought from the recipient that the sensitivity of the information is understood and appropriate protection is available.
- Copying should only be carried out with the permission of the information owner and should only be carried out by staff who themselves are authorized to see and handle information with this level of security. Care must be taken to ensure that additional or spoilt copies are destroyed. There should be clear distribution lists with numbered copies and they could also be marked 'Not to be copied further'.
- SEC material should be stored under conditions that make accidental compromise unlikely, offer a degree of resistance to deliberate compromise and make actual or attempted compromise likely to be detected. It is practical to display a warning that any compromise will be detected and violators pursued. The way in which the material is handled, used or transmitted should make accidental or deliberate compromise unlikely.
- When not in use, the physical material should be locked in approved security containers, within a managed security perimeter. A clear desk policy should be rigidly enforced.
- IT systems, within a managed security perimeter, should be strongly secured with approved access controls that are highly resistant to penetration by a capable hacker. Highly effective monitoring procedures should be in place to detect unauthorized access.
- Discussions of information with this level of security should take place only where there is no likelihood of being overheard or monitored by surveillance equipment.
- Mail should be sealed and sent in a way that ensures that its sensitivity level is not apparent from the envelope. There should be safeguards to prevent and detect attempts to read the information. It should therefore be delivered by a trusted individual or an approved courier in a double-sealed envelope and there should be a receipt for it.

- Faxes should only go over secure connections, and telephone conversations should only take place over secure links. Steps should be taken to ensure that neither party to such a conversation can be overheard.
- IT systems should be fully physically secure and any messages sent via the internet (e-mail, instant messenger, etc) should be encrypted. Information should not be stored on a network that is connected to the internet, however strong the firewall connection.
- Destruction of SEC3 material should be done in a way that makes attempted or actual compromise, accidental or deliberate, unlikely, reconstitution difficult and any attempted compromise likely to be detected. Destruction should be recorded.
- Hard disks should be overwritten with a secure approved utility. Media (eg USB sticks) that are to be destroyed should be destroyed by an approved company and their destruction recorded. All back-up copies and files also have to be destroyed.
- Home working facilities should be organizationally approved and appropriately secured.
- This sort of information should never be discussed on planes or other forms of public transport or where any non-trusted person is present. It should not be discussed in public places, hotel rooms, competitors' premises or restaurants.
- Notebook computers carrying this information should be kept secured to SEC3 standards at secure offices and kept supervised at all times. They should not be left in taxis or airports or anywhere else.

Non-disclosure agreements and trusted partners

There will be circumstances where the organization needs to share confidential information, of either an SEC2 or an SEC3 level, with a third-party organization. This might be as part of a series of commercial negotiations or other important circumstances. An appropriate risk assessment should be carried out prior to sharing any information with the third-party organization, and the results of this risk assessment should be reflected in a non-disclosure agreement (NDA) that the third party is asked to sign. The NDA should be drafted by a legal specialist and should include the appropriate controls identified for dealing with suppliers and in this chapter. The controls should be selected to ensure that the third-party organization is

able to respect the information security classification that has been assigned to the material to be shared. The majority of the controls that should be listed in the NDA will be drawn from the list of information handling requirements shown in this chapter, and some controls for third-party contracts, where the risk assessment identifies them as necessary. No information should be released until the NDA has been signed by the appropriate authority in the third party and returned.

Those organizations that do have to share confidential information regularly will have a well-developed procedure for carrying out these risk assessments (probably based on a standard questionnaire drawn up by the internal information security adviser) and a standardized but customizable NDA. This should enable the process to be completed expeditiously; the organization will certainly want to ensure that it can be dealt with quickly and effectively, as otherwise either the information will be shared without safeguards or the organization will struggle to achieve its own objectives.

Asset handling procedures

Control 8.2.3 of ISO27002 says the organization should establish asset handling procedures, in line with its classification system, that will protect its information from unauthorized disclosure or misuse. These procedures should apply to all information assets documents, computing equipment, networks equipment, mobile devices, removable media, etc. The control requires the organization to do a number of things that it has already tackled under other headings, and one or two new ones. As a starting point, information should be labelled and handled consistently with its classification (see above), irrespective of the media that contain it. In addition, ISO27002 recommends that the procedure should cover:

- Media in transit.
- Access restrictions to identify unauthorized personnel.
- A formal record identifying authorized recipients of data, which lines up with the classification of the data.
- Ensuring that media are stored in line with manufacturers' recommendations, which are usually common sense.
- Keeping data distribution to a minimum, in line with their classification, and clearly marking all copies of media for the attention of the authorized recipient.

10

Media handling

Control objective A.8.3 of the standard seeks to prevent damage to, disclosure or unauthorized removal or estruction of any of the organization's information which is stored on removable media; by definition, therefore, this control is also interested in protecting the media and protecting the organization from any disruption to its business activities. It has three controls, dealing respectively with managing removable computer media, disposal of them, and procedures for managing their physical transfer.

Management of removable media

Control 8.3.1 of ISO27002 says the organization should control removable computer media, such as external hard drives, USB sticks, tapes, disks, cassettes and printed reports, so as to prevent damage, theft or unauthorized access. ISO27002 recommends that documented procedures should be included in the ISMS as follows:

- It should be required that the previous contents of any reusable media that are to be removed from the organization should be erased. The erasure must operate across the totality of the media, not simply across what appears to be the existing content, as otherwise there is a danger that information may leak to the outside world.
- Authorization should be required for all media that are to be removed from the building, and an audit trail should be retained. Some media, such as back-up tapes, are removed on a daily basis, and the authorization for such standard removals should be documented in the ISMS. Other media, such as USB sticks, are more easily portable (and can also introduce threats such as malware), and the organization's overall policy on these will need to be determined.

- All media should be securely and safely stored in line with the manufacturer's recommendations. Media safes that have an appropriate fire resistance should be installed, in line with the guidance set out in Chapter 10. Library procedures should be considered to ensure that media are properly tracked and controlled.
- Information that is likely to be required at some point beyond the media lifetime (check the manufacturer's statement about media longevity) will need to have appropriate arrangements made to ensure its future availability – including alternative storage, so as to avoid the impact of media degradation.
- Of course, removable media should only be allowed if there is a genuine reason for doing so and, where there is, all the risks associated with it going missing should be considered – dealing with these risks might include cryptography, alternate copies of media, secure storage of critical media and, finally, staff training: if a member of staff downloads confidential information, such as PII to an unencrypted USB stick and then drops it in a public car park, someone (usually a news reporter) will find it and there will be problems!

Disposal of media

Control 8.3.2 of ISO27002 says the organization should have formal procedures for the secure and safe disposal of media when they are no longer required. Careless disposal of media (which includes throwing disks or CD-Roms into waste bins or losing USB sticks) could enable confidential information to leak to outside persons. There should be documented procedures in the ISMS that ensure disposal is done securely.

The items that should be considered for secure disposal under such a procedure are paper documents, voice or other recordings, old technologies such as carbon paper, output reports, one-time printer ribbons, magnetic tapes, as well as more recent media such as removable disks, USB sticks or CD-Roms, optical storage media, program listings, test data and system documentation. Media such as these, containing sensitive information, should be disposed of securely. Some organizations may wish to separate media that carry sensitive information from those that do not, and will need to carry out a risk and practicality assessment to decide how to deal with them. Other organizations will simply treat all disposable media in the same way, so as to avoid any risk of sensitive data bypassing secure disposal

arrangements. This means shredding or incineration or, for magnetic media, overwriting. It is usually sensible for all media to be gathered together and disposed of simultaneously rather than attempting to separate out sensitive media. The best way to do this is through a series of disposal bins and baskets, located throughout the organization's premises, into which identified types of media go when they are no longer required. A specialist contractor would normally supply these bins and the associated removal and destruction service. Contracting with such an organization should obviously be subject to the disciplines normal for supplier management. A log of disposals should be maintained.

Physical media in transit

Control 8.3.3 of ISO27002 says the organization should protect from unauthorized access, misuse or corruption any media being transported beyond the organization's physical boundaries. You should bear in mind that a back-up tape, for instance, is a different asset from the original information; it should be subject to its own risk assessment and its own risk treatment plan, taking into account its sensitivity, criticality, etc.

As USB sticks and back-up tapes are among those media most regularly transported, and as the organization's survival could depend on their protection, it is particularly worth getting this right for these media. The mail and casual courier services are not necessarily secure transport services. There are a number of controls, the benefits of which are self-evident, that ISO27002 recommends should be considered in relation to the security requirements for the media in transit:

- Encryption should be considered, particularly where the media contain personal or sensitive information.
- A list of authorized, reliable and trusted couriers should be established, and contracts following the standard pattern should be negotiated. The contract should include some method by which the organization can satisfy itself as to the background checking processes applied by the courier company to all its staff, particularly its temporary and part-time staff. There should be an agreed method of identifying the courier on arrival at the dispatching organization, and obtaining signatures for the media.
- Packaging of hardware should be in line with manufacturers' specifications and, in any case, sufficient to protect the contents from any likely physical

damage, including environmental factors such as heat, moisture or electromagnetism.

- Where necessary, appropriate physical controls should be adopted to protect particularly sensitive information. These could include delivery by hand, the use of special locked containers (with keys sent by alternative routes), tamper-evident packaging, split deliveries (so that neither single delivery will give the whole story) and use of advanced cryptographic controls.

11

Access control

Control objective A.9 of the standard is extremely important; it focuses on access to information, and a properly thought-through and thoroughly implemented access control policy, within the ISMS, is fundamental to effective information security. This control category provides for appropriate monitoring and is a major clause in the standard and a major component of the ISMS.

The reader needs to understand that access control has become increasingly critical over recent years. Chapter 1 set out the key reasons why cybercrime is on the increase and outlined the nature of the advanced persistent threat facing most economies today. In particular, it pointed to the growth in hacking. It is worth understanding the world of hackers, as a background to the need for effective access control.

Hackers

It has been argued that hackers have four prime motivations:

- challenge – to solve a security puzzle and outwit an identified security set-up;
- mischief – wanting to inflict stress or damage on an individual or organization;
- working around – getting around bugs or other blocks in a software system;
- theft – stealing money or information.

Hackers like to talk about 'white hat' and 'black hat' hackers, or just 'hackers' (good) and 'criminal hackers' (not so good). The argument is that the 'black hat' hackers are malicious and destructive while the 'white hat'

hackers simply enjoy the challenge and are really on the side of good, offering their skills to help organizations test and defend their networks. This differentiation is convenient for hackers, who seem able to change hats as easily as they would evade network defences. The only sensible approach for any security-conscious organization is to assume that all hackers are potentially in the wrong-colour hats, however they might initially present themselves. 'Grey hats' is a term that has evolved to recognize the uncertain danger of so-called 'ethical' hackers.

The 'Certified Ethical Hacker' (CEH) certification is one of a growing range that have evolved to recognize a particular level of hacking skill, based on completion of an intensive training course. Those who go on such a course are not initially screened for their ethical bias, and one should approach the employment of a CEH with open eyes. Of course, the absence of a formal qualification should prevent one from hiring anyone to test network systems.

The term 'cracker' evolved to identify black hat hackers who break into computer systems specifically to cause damage or to steal data. Hackers like to say that crackers break into computers but that hackers get permission first, and will publish their discoveries. Of course, hackers become crackers, crackers become hackers, and either could become a security consultant.

'Script kiddies' are none of the above; most IT departments contain one or more individuals whose interest in testing the systems that they are employed to protect leads them from time to time beyond the law. They are not as sophisticated as hackers and so they have not yet qualified for a hat, but, using their own very simple code or, more usually, programs found on the internet, they can be just as lethal to unprotected systems as the higher profile hacker collectives that have gained press coverage in direct proportion to their hacking exploits.

Hacker techniques

Some of the more common, basic techniques that hackers use to gain access to networks are set out, alphabetically, below. The OWASP Top 10 are the most significant web application vulnerabilities, and the SANS Storm Centre releases updates on new, critical vulnerabilities. The list, which includes common hacker terms, keeps growing and is therefore never up to date:

- **Abusing software.** Hackers, once they have gained access to a system, use the installed software for their own ends. This can include using

administrative tools for uncovering network weak points for exploitation, abusing CGI (Common Gateway Interface) programs on web servers, exploiting vulnerabilities in Microsoft's Internet Information Server (IIS), and so on. The advice of a network security specialist should be sought to ensure that the organization fully understands the current level and type of risks arising from these types of activities.

- **Back door.** Programmers or administrators deliberately leave ways into software systems that can be used later to allow access to the system while bypassing the authorized user file. Sometimes, developers forget to take out something that was put there simply to ease development work or to assist with the debugging routine. Sometimes ways are deliberately left in to help field engineers maintain the system. However they get there, they can provide any unauthorized user with access to the system.
- **Back orifice.** This program is a remote administration tool that has great potential for malicious use. It is very easy to use, so that script kiddies have no problem using it. It is also 'extensible', which means that it develops and improves with age. Most anti-malware systems should detect and remove back orifice, but new versions become available on a regular basis.
- **Broken authentication and session management.** These attacks take advantage of flaws in areas such as logout, password management, timeouts, remember me, secret question, account update, etc to impersonate users and take over privileged accounts.
- **Buffer overflow.** A buffer is an area of memory that holds data to be processed. It has a fixed, predetermined size. If too many data are placed into the buffer, they can be lost or can overwrite other, legitimate data. Buffer overflow vulnerabilities have for a number of years been a major source of intrusion. They provide hackers with an opportunity to load and execute malicious code on a target workstation.
- **Cross-site request forgery (CSRF).** This takes advantage of web applications that allow attackers to predict all the details of a particular action. Since browsers automatically send credentials such as session cookies, attackers can create malicious web pages that generate forged requests that are indistinguishable from legitimate ones.
- **Cross-site-scripting (XSS).** This is the most prevalent web application security flaw and attackers attempt to exploit it by executing scripts in a victim's browser to hijack user sessions, deface websites, insert hostile content, redirect users, hijack the user's browser using malware, etc.

- **Denial of service (DoS).** This sort of attack is designed to put an organization out of business for a time by freezing its systems. This is usually done by flooding a web server with e-mail messages or other data so that it is unable to provide a normal service to authorized users. A distributed denial-of-service (DDoS) attack uses the computers of other, third-party organizations or individuals (which have themselves been commandeered by the cracker) to mount the attack.
- **Exploit.** This is either the methodology for making an attack against an identified vulnerability (the noun) or the act (the verb) of attacking or exploiting the vulnerability. Exploits are often published on the internet, either by black hats or by grey hats, who claim that this is a good way of forcing software suppliers to develop more secure software or to provide fixes for existing software.
- **'Man in the middle'.** A hacker places himself or herself, undetected, between two parties to an internet transaction, whether on a local area network (LAN) or on an unsecured internet link. The hacker intercepts and reads messages between the two parties and can alter them without the intended recipient knowing what has happened. This is often recognized as a form of masquerading (see below).
- **Masquerading.** A hacker will pretend to be a legitimate user trying to access legitimate information, using a password or PIN that was easily obtained or copied, and will then try to access more confidential information or execute commands that are not usually publicly accessible.
- **Network monitoring.** This is also known as 'sniffing' and involves deploying some code on the internet to monitor all traffic, looking for passwords. These, and other ostensibly confidential information, are often sent 'in the clear', and therefore can easily be located and written to the hacker's workstation for future use.
- **Password cracking.** This is actually, on balance, very easy. Most users do not set up passwords or, if they do, use very simple passwords that they can easily remember, like 'secret' or 'password', or their children's names, or birthdays, sports teams, particular anniversaries or family names. While some hackers can quickly identify particular users' passwords, software is now available on the internet that will apply 'brute force' to try, automatically and at high speed, every theoretically possible alphanumeric combination of user name and password and, usually aided by a dictionary of common passwords, this can quickly enable a

hacker to gain access to a system. Once a hacker locates the list of encrypted passwords on the security server, he or she can use internet-available software tools to decrypt it.

- **Polymorphic attacks.** The polymorphic attack uses advanced techniques to obfuscate the malicious code that is executed when an attack successfully takes advantage of a system's vulnerability to compromise the system. They continuously change (or 'morph') non-essential components of their code, while maintaining the core attack algorithm, to deceive intrusion detection systems.
- **Rootkit.** Originally, a rootkit was a set of tools that allowed administrator-level access (called 'root' access in the Unix world) to a computer or network. These tools could also be used by an attacker to hide evidence of his or her intrusion. The term has therefore evolved to describe stealthy malware – malware such as a Trojan, virus or worm – that actively conceals its existence from computer users and system processes.
- **Security misconfigurations.** These can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code. They enable attackers to access default accounts, unused pages, unpatched flaws, unprotected files and directories, etc to gain unauthorized access to or knowledge of the system.
- **'Social engineering'.** The easiest and most common method of gaining access to a network or secure environment is to trick someone into providing confidential information. The hacker, for instance, poses as a network administrator or a fellow employee with an urgent problem that can only be resolved by the employee providing confidential information (such as user name or password). Alternatively, the hacker has a false business card, claiming to be a key technical or business support representative, or claims to be a new employee trying to get up to speed in the business. Staff should not divulge their password to anyone, even IT support staff. For emergency access to restricted systems and administrative applications, the information security manager may want to hold administrator passwords in a central password manager. Irregular testing needs to occur so that should an administrator be dismissed for any reason, the system(s) to which he or she had access can be maintained, and the passwords changed.
- **Spoofing.** IP spoofing gains unauthorized access to a system by masquerading as a valid internet (IP) address. Web spoofing (phishing

and pharming) involves the hacker redirecting traffic from a valid web address to a fraudulent, lookalike website where customer information (and particularly credit card information) is captured for later illegal reuse. Phishing is also the attack vector of choice for deploying malware onto networks.

- **SQL injection.** This is inputting SQL statements into a web form, trying to find design vulnerabilities that will allow the hacker to write directly to the database to change or extract the data.
- **Trojan horses.** These are programs that, while they might appear to be useful utilities, are designed secretly to damage the host system. Some will also try to open up host systems to outside attack.
- **Zero Day attacks.** These occur when a flaw in software has been discovered and exploits of the flaw appear before a fix or patch is available. Once a working exploit of the vulnerability is released into the wild, users of the affected software will be compromised until a software patch is available or some alternative mitigation is put in place.

Hackers do not exist only outside the organization. They are often employed by the organization that they target. They might also be disgruntled former (or about to be former) employees who want to take revenge on the organization for letting them go. Internal hackers can be more dangerous than external ones, not least because they start off knowing far more than anyone outside the organization. They might already have access rights that are capable of getting them to places that the organization does not want them to visit. Equally, it is possible for an attacker to gain unauthorized access to the organization's premises and, once inside the physical perimeter, to access a relatively unsecured machine through which the entire network can be reached. The fact that an information system is not directly connected to the internet does not mean that it is not liable to be attacked. Such systems have to be subject to the same level of security as those that are connected to the internet, and the risk assessment needs to take all possible risks into account.

System configuration

The first step that any organization should take in order to deal with the threat of hacking is to eliminate as many as possible of the vulnerabilities that may be native to the Microsoft (and other) software packages deployed in the workplace. This is done by ensuring that the systems are loaded

and configured in line with the Microsoft guidelines (as set out at www.microsoft.com/en-gb/security (archived at https://perma.cc/YY9A-6W65)) and as amended or strengthened by the recommendations set out on the website of the CERT coordination centre (www.sei.cmu.edu/about/divisions/cert/index.cfm (archived at https://perma.cc/C9ZJ-KUQ7)), the Software Engineering Institute of the Carnegie Mellon University. Their configuration recommendations are independent and, subject to the organization's own risk assessment, their recommendations ought to be adopted as basic good practice in server and workstation configuration.

Whatever technical requirements are adopted by the organization, they should be documented and appropriate steps taken to ensure, by means of a regular independent technical check, that they are being maintained.

Access control policy

Control 9.1.1 of ISO27002 says the organization should define and clearly document its access control policy on the basis of business and information security requirements and then to restrict access to what is defined in the policy. Access controls are both physical and logical, and, as they should complement each other rather than conflict, they should be considered together. This consideration has to take into account the range of risks from hackers and crackers, and, if necessary, specialist advice on the latest cracker threats and technological defences should be taken as part of the risk assessment process.

Access control rules and user rights for individual users and groups of users should be related to business objectives and clearly documented, and users should be aware of them. Failure to implement the policy properly will lead to too many people having access to too much information and at too high a level of confidentiality. This tends to lead to unauthorized access to information, disclosure to third parties of confidential information, etc. Training on the access control policy and access control rules should be part of basic user training. The level of dependency on other, highly individualized components of the ISMS means that each organization has to develop its own unique policy.

The access control policy in the ISMS should, ISO27002 says, take a number of factors into account:

- Different business applications have different security requirements. These are determined by identifying all the information that the business

systems are carrying and through the individual risk assessments carried out for each critical business system; these risk assessments point at who should, and should not, be allowed access to the system.

- Some information required for particular business applications may be processed by people who do not need access to the application itself (the 'need-to-know' principle in action). An example might be in an office workflow system, where the person who inputs a supplier delivery note to a purchase and payments application does not need access to the actual accounting or payment functions of the system. Such a person would need different access rights from those required by a person who triggers actual vendor payments.
- The information classification system needs consideration. User access rights should reflect the level of information that users are allowed to see.
- There should be consistency between the access control and information classification policies of different networks within the same organization; inconsistency leads to incoherence, which leads to people taking short cuts (because of there being an excessive number of user names and passwords, and too much variation in responsibility), and this leads quickly to breakdowns in information security.
- Relevant legislation, particularly data protection legislation, and any contractual obligations that the organization has to protect particular data should be analysed and taken into account.
- There should be standard user access profiles for common job categories, as this makes it straightforward to manage and provide training. In situations where people with similar jobs have different access rights, security will break down as individuals unofficially share the most useful access profiles. Authorization to create a new user name should set out the areas of the network to which the user is to have access.
- A distributed, networked environment that recognizes a number of different types of connections should consider all of them, so that, for instance, a user who can access something on the desktop can also do so remotely. The Microsoft Windows roaming profile makes this possible.
- Segregation of duties should apply here as well: if the organization is large enough, different roles should be responsible for processing access requests, authorizing them and setting them up.
- Access controls, like all ISMS controls, should be periodically reviewed; as a weakness in this control could provide access to sensitive and

confidential information or systems, it is as important to monitor this as it is to monitor the activity of those who have access to the organization's bank account.

- Access rights should be formally approved, regularly reviewed and removed or adjusted when an employee is terminated or has a change of role. (This aspect, covered by control A.9.2.6, was dealt with in Chapter 8.)

The access policy will set the key principles that are to govern access to information and information systems. In setting these rules, the ISMS must clearly differentiate between rules that are always enforced and those that are optional, conditional or occasion specific. A key principle should be that whatever is not expressly permitted is forbidden; the alternative, that what is not expressly forbidden is permitted, is much weaker and can, for instance, allow hackers on the organization's staff full licence to indulge in whatever they think they can describe as being not forbidden.

Changes in information classifications, in user permissions and in access control rules (and these can happen both automatically through the system and as a result of human intervention, some of which may or may not require other approvals before implementation) should also be considered in drawing up the detailed rules. The overall objective must be to identify and close loopholes in the rules as early as possible. Regular review of access control rules is therefore very important.

Network Access Control

Network access control needs to be considered in the context of the changing access needs of users and organizations. Accessibility of internal and external networked services should not compromise the security of those services. This means there need to be appropriate interfaces between the organization's network and other networks, particularly the internet, with appropriate authentication mechanisms for users and equipment, and controls over user access to information services.

A private network that carries sensitive data needs to protect the privacy and integrity of that traffic. When such a network is connected to other networks, or when browser access is allowed, the remote terminals and other connections become extensions to that private network and must be protected accordingly. In addition, the private network must be protected

from outside attacks that could cause loss of information, breakdowns in network integrity or breaches in security.

There is more to the issue of network security than simply considering fixed private networks, whether local area networks (LANs) or wide area networks (WANs). WANs and LANs are usually discrete networks using fixed private cabling within the organization's facilities to connect their information processing facilities (a LAN) or using privately leased or owned fixed data links to connect LANs in a number of different locations securely. Virtual private networks (VPNs), extranets and wireless networks are now important parts of the networking universe.

Virtual private networks (VPNs)

VPNs are, in effect, alternative WANs that replace or augment an existing fixed private network. There are two types of VPN: remote access VPNs, which extend the network to telecommuters, home offices and mobile workers, enabling them to log on securely to the corporate network across the internet; and site-to-site VPNs, which securely connect remote sites to a corporate or central site, using service provider connections or the internet. A VLAN is a group of end stations which, independent of physical location, are networked by means of a VPNs. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN.

VPNs utilize specific technologies, such as Internet Protocol Security (IPSec), which takes advantage of digital encryption technology. VPN technology has become relatively ubiquitous, but installation of a VPN may require specialist technical advice as well as the specialist technology. The organization will need to carry out a risk assessment in respect of its VPN, expecting that it should employ the same security and management standards for its VPN as for any fixed network.

Extranets

Extranets support business-to-business (b2b) commerce and collaboration between independent entities, typically via the internet. As markets consolidate and core services are externalized, organizations need to communicate securely with a network of external partners that includes outsourcing companies, demand and supply chain partners, consultants and contractors. Extranets need to be extremely flexible and must be deployed quickly (in

'internet time') without needing to redevelop or re-architect existing applications while leveraging existing infrastructures. They must also be scalable, to allow for future growth to be supported quickly, easily and inexpensively. At the same time, extranets must ensure that confidential information remains confidential and that authenticated users can access only the services they are authorized to access. This needs to be done without requiring the partner, customer or vendor to change its security policies, network infrastructures or any aspect of its existing set-up for the benefit of the extranet.

This appears to fly in the face of the requirements of ISO27001; however, organizations need to respond to market drivers without compromising their information security. Extranets should be deployed in line with business objectives; there is no such thing as a 'one size fits all' extranet. Some extranets are designed for user groups simply to view static information, while others are designed for a more dynamic interaction with the enterprise. The extranet might need to communicate with a mass of customers, or a mass of suppliers, or a small number of partners involved in product development or some combination of these.

Secure extranets will rely on encryption, strong two-factor or even multi-factor authentication, granular access control and other VPN security features. The extent to which third parties can effectively be bound by contracts is limited by the extent to which their terms can be accepted at the initial log-in stage of accessing the extranet. There are specialist products that can be deployed to create and manage secure extranets, or organizations can create their own simply by implementing the types of security solution discussed in this book. The management process is the same for extranets as it is for other information security issues: carry out a risk assessment and deploy an appropriate, cost-effective solution.

NIST's Special Publication 800–47, Security Guide for Interconnecting Information Technology Systems, provides guidance on planning, establishing, maintaining and terminating interconnections between independent organizational information systems. It can be accessed at csrc.nist.gov (archived at https://perma.cc/Z5WL-42XB).

Wireless networks

Wireless networks are an increasingly important issue, in information security terms. Wireless networks are convenient, inexpensive to set up (there is no category five fibre optic cabling to lay or move) and they enable group working and data sharing to take place easily and simply. They consist of

notebooks, workstations, mobile devices and other peripherals that access a corporate network using shared radio waves, wireless access points and wireless networking protocols. The WEP (Wired Equivalent Privacy) and the 802.11 group of standards were created to tackle the vulnerability that comes from using shared radio waves to transmit data, in theory making wireless transmissions as safe as using a fixed network by encrypting wireless traffic and using WEP to authenticate nodes.

However, many wireless networks have no security, WEP is extremely limited as a security technology, and wireless networks are extremely vulnerable. Flaws continue to be found (by 'war drivers' and 'war chalkers' and wireless hackers), which means that the wireless security standard is continuing to evolve, with WPA (wi-fi Protected Access), WPA2 and 802.11i the current security standards. Specialist security procedures will be necessary for wireless and networks mobile workers. These include advanced encryption key management and, more significantly, placing the wireless network outside the organizational firewall, with no routes to the outside internet other than through a secure VPN. A detailed risk assessment drawing on specialist advice that reflects the risks of bandwidth theft, security gateway bypassing, identity theft, illegal activity and espionage should inform the decision on this issue.

There are a number of other basic security requirements in regard to wireless networking that should be put in place as a matter of course. These include changing the SSID (Service Set Identifier – the public name of a wireless network) to one that does not identify its location or users, ensuring that access control is enabled, as well as requiring WPA or WPA2. Network administrators should, subject to their risk assessment, have a process for monitoring whether or not mobile wireless access points have been plugged into their network.

These sorts of wireless networks are not, however, the end of the story. Wireless networking includes the increasing array of machines that are designed to access corporate networks other than across fixed links. There is, of course, the mobile phone. Smartphones themselves carry large amounts of important contact information, and retained data, voice and text messages make them potential targets for attackers. Mobile devices, which are able to remotely access corporate networks are becoming more popular with hackers and virus writers as a route into otherwise well-defended networks.

Bluetooth is a wireless protocol built into a widening range of products to enable short-range wireless data communication between equipment and with Bluetooth hubs. Voice communication with computers, and voice over

IP (VoIP) technology, are becoming more and more effective. All of these technologies have real vulnerabilities and pose real security threats to organizations, from airborne virus infection to data loss and unauthorized network access. These tools will, however, continue proliferating because they improve the productivity of workers and the interconnectedness of data. Banning these tools will not be an effective solution for organizations. Information security advisers will need to keep themselves abreast of developments and will have to become adept at carrying out risk assessments on new technologies and on finding appropriate security solutions to the vulnerabilities and threats that are thus identified. Specialist advice may be necessary on a regular basis, and organizations may decide that, as a matter of policy, they will not adopt new technologies for a defined initial period during which they hope that their vulnerabilities will be identified and solutions to them found. NIST's paper SP 800–48, Security for Wireless Networks and Devices, at https://csrc.nist.gov, (archived at https://perma.cc/Z5WL-42XB), provides a good technical overview of the security issues.

The essential starting point for tackling the network access part of the ISO27001 exercise is a network map that shows clearly all the assets on the network, and all their connections, whether internal or external. It should also show any wireless connections and any related domains, including certainly any demilitarized zones (DMZs) and extranets. A series of risk assessments is then carried out in respect of each of the external connections, and appropriate controls, selected from those identified by ISO27002 are selected to deal with the assessed risk.

Access to networks and network services

Control A.9.1.2 says the organization should design and implement a policy, within its ISMS, that ensures that users have access only to the services that they have been specifically authorized to use. The policy should identify which networks and network services are allowed to be accessed, the authorization procedures necessary prior to any such access, and the controls necessary to protect access to network connections and network services – which should extend to how the means of accessing these networks are controlled. This policy should be consistent with the access control policy discussed in relation to A.9.1.1 and should recognize and allow for the future evolution of networking technologies in a way that provides guidance to the organization on how to respond securely to these changing circumstances. This all means that users should see, on their desktops, only icons

for those services that they are authorized to access; no information should be provided about other services that are on the network, as attempts to crack into them should not be encouraged.

Firewalls and routers are key components of the network security perimeter.

Firewalls and network perimeter security

Network perimeter security controls access to the network so that only authorized users can access applications, data and services running on the network. Firewalls are generally the first security product that organizations deploy to protect their network perimeters. A firewall provides a barrier to traffic seeking to cross the perimeter and permits only authorized traffic to pass, in line with a predetermined access policy. Firewalls will also usually provide some level of network address translation (NAT) services, denial-of-service (DoS) attack protection, IPSec VPN services and intrusion detection services. A perimeter firewall may also need to integrate with device-level firewalls on mobile laptops and smartphones.

There are a large number of firewalls available, and the organization should research the market thoroughly before making its choice. In general, vendors that have been in the business for some years and that clearly have resources adequate to maintain the development of their products should be favoured. It is important that the chosen anti-malware software should be able to work with the preferred firewall. At the same time, and bearing in mind the speed of change in the security market, current security sites (see Chapter 4) should be consulted to establish which firewall products are proving easiest for hackers to conquer or most inadequate for current performance requirements.

Once the firewall has been chosen, the policies that it is to apply will need to be selected and documented in a way that reflects a specific risk assessment. It is important that these are chosen as the result of an informed risk analysis that is in line with the organization's access control policy, as otherwise it will find itself unable to operate effectively. There are internet resources that the organization needs, and the safest perimeter policy, which is simply to close all ports on the firewall, is not necessarily the most sensible. As usual, specialist technical advice, combined with current information about security vulnerabilities and threats derived from vendor and independent websites, may be necessary for the correct configuring of the firewall.

NIST has a Special Publication, number 800–41, titled *Guidelines on Firewalls and Firewall Policy*. The document contains guidelines on configuring and administering firewalls as well as covering related issues such as VPNs, web and e-mail servers and intrusion detection. It contains links to other firewall-related resources. The NIST website is at https://csrc.nist.gov (archived at https://perma.cc/Z5WL-42XB).

The firewall and its correct configuration can be business-critical for any organization, and the vendor's default password (which will be widely known) must be changed. An ISO27001 auditor will therefore want to see evidence that managers have reviewed the firewall configuration. Any subsequent changes to the rules agreed for the firewall need to go through the same authorization process, with evidence available to prove this, and not be implemented at the whim of a system administrator.

Routers and switches

In addition, the organizational network infrastructure should be built using routers and switches that themselves have adequate security features. The selection of routers and switches should be subject to the same level of care as was the selection of a firewall, and, while these are technically simpler devices, they too can provide an attacker with a way into the network. Routers and switches should be configured in line with the manufacturer's recommendations (including changing the vendor's default password) and have correctly configured and up-to-date access control lists (ACLs). ACLs ensure that only legitimate users can pass through the router or switch. Routers and switches can also have core firewall technology embedded in them, and the choice of which switches and routers to deploy should be made in the light of a risk assessment and a review of independent assessments of vendor products.

Organizations with larger networks should also consider technology solutions that enable them centrally to define, distribute, enforce and audit security policies for a large number of routers, switches and firewalls. Cisco, for instance, provides technology solutions that specifically enable this type of centralized security control. The larger the network, the more important – and cost-effective – such a solution is. In addition, larger organizations should consider (in the light of the risk assessment) deploying intrusion detection systems (IDSs) that can monitor and reactively respond to intrusions as they occur, and network vulnerability scanners that proactively identify areas of weakness. These are important because while firewalls

provide an enforced path control for external users, they do not actively analyse the traffic for attacks or search the network for vulnerabilities. In particular, firewalls do not address the threats posed by insiders. IDS packages can be sourced through major vendors of security products and through the security sites on the internet. In considering IDS packages, the total cost of ownership will be important, and the organization must be clear on how it will deal practically with the output of the detection system. There should also be regular scans of the network for the existence of unauthorized wireless access points.

Large organizations, or organizations that need to run large networks or complicated mixes of services dealing with a complex web of partners, customers and vendors, should consider constructing the network as a whole. This will require the input of a network specialist, and the organization chosen to provide this service should be able to point to similar solutions successfully implemented for similar clients elsewhere. Large networks might be segmented, or compartmentalized, structured around a number of separate logical domains, as a method of limiting the extent to which an intruder can affect the entire network.

Network intrusion detection systems (NIDS)

A network intrusion detection system is hardware or software that automates the process of monitoring events in systems or networks to detect intrusions. An intrusion is an attempt to break into or misuse an information system, or bypass its security controls, in order to compromise the confidentiality, integrity and availability of information stored on it.

There are different types of intrusion detection systems. A NIDS, also known as a 'network sniffer', monitors packets on the network and attempts to discover if a hacker is attempting to break into the system (or cause a denial-of-service attack). A system integrity verifier (SIV) monitors system files to find when an intruder changes them so as to set up a back door. Log file monitors (LFM) monitor log files generated by network services. In a similar manner to NIDS, these systems look for patterns in the log files that suggest that an intruder is attacking. There are a number of products that perform these various tasks and that can be quickly and easily identified through a product search. Use of such a product should be as the result of a risk assessment, and its use should be planned alongside any other network monitoring and anti-malware tools that the organization chooses to deploy.

Reference should also be made to the NIST publication SP 800–31, *Intrusion Detection Systems,* which can be accessed on the NIST website (see above).

User authentication for external connections

It would make sense for the organization to ensure that access to its network by remote users is subject to authentication. A risk assessment should be the basis of selecting an appropriate remote access authentication control; clearly, the existence of any dial-up or wireless access to the network offers attackers a potential way into it. There are a number of approaches and technologies that might, depending on the risk assessment, be appropriate.

The most straightforward methods of authenticating remote users include RADIUS (Remote Access Dial-In User Service), TACACS+ and Kerberos protocols, combined with CHAP and PAP protocols, which are the foundation of secure remote access across the internet. Strong, two-token authentication is also an effective component of remote access authentication, and there are a number of vendors that provide effective services based on these technologies.

Dedicated private lines or facilities for checking network user addresses can be used to provide assurance that the source of the connection is trusted. Equally, dial-back procedures and controls (eg by enabling the modem dial-back facility on a remote access service) can provide protection against unauthorized connections, although, to be secure, these controls should not be used where network services provide call forwarding (now available on most modern telecommunications services). Call-back processes must happen only after the incoming call has been disconnected, and thorough testing should be carried out to ensure that this control actually works.

Node authentication is an alternative method of authenticating connections to remote computer systems. These might be the computer systems of partners, vendors or other third parties. Where a remote computer accesses another computer system, it is authenticated following one of the controls (other than hardware or two-token authentication, which is designed for human users) such as a cryptographic one identified above. This is to ensure that the automatic connection to or from a remote computer does not provide a way of gaining unauthorized access to a business application. A risk assessment should identify the critical nodes and be used to justify the level of control implemented.

12

User access management

Control category A.9.2 of the standard deals with unauthorized access to information systems. Its six controls focus on how user access is set up and how access rights to systems are allocated and managed. It is not appropriate for user access policy to be created and solely managed by either the IT depart- ment or the HR department.

It is important to have an overview of the current user authentication technology. A few years ago, it was a reasonable assumption that anything outside the network perimeter was dangerous until proven otherwise, but that anyone within the network perimeter could be trusted. While network defences continue to be crucial, in the age of the porous perimeter it is now the case that virtually anyone can interact with the connected organization's computers, from business partners accessing the extranet to customers accessing the public e-commerce website. It is no longer the case that anyone who has successfully logged on to the network is necessarily a trusted party.

Security technology has evolved to reflect this change and, increasingly, concentrates on application-oriented and endpoint security as distinct from whole-network security, so that each critical resource, application or device on the network has, and can enforce, appropriate security policies.

For the purposes of this chapter, the related – but different – concepts of user authentication and user identification are fundamental. User authentication is establishing the authenticity of a user in the context of a computer-based interaction. There are three main approaches.

The first is to use a password, or some other information (such as mother's maiden name) that in theory only the user would know. This is the easiest approach and also the easiest to subvert, as a result of which password protection has become inadequate for sensitive information

and resources. There are two technology protocols that handle password authentication, TACACS+ and RADIUS. The latter is an Internet Engineering Task Force (IETF) standard and is increasingly accepted by companies providing internet services; it is used in conjunction with strong authentication (see below). Systems should use one or the other protocol and should process authentication requests using CHAP (Challenge Authentication Protocol) before it falls back to using the less strong PAP (Password Authentication Protocol), set up to use the option of encrypting passwords in transit, before rejecting a user as invalid.

The second approach is to require the user to present proof via something physical, most commonly a dedicated authenticator that generates access codes (usually called a 'token'), a smart card, special authentication software or a digital certificate. Codes can be generated centrally and sent to users by text. Tokens that generate a changing numeric authentication code each minute are popular. The security server is able to confirm that the currently valid code is the one shown on the token, and the presence of the valid code plus the user's password is usually taken as adequate authentication of the user. This form of two-factor authentication becomes more prevalent as the cost of producing the tokens benefits from economies of scale, even though authenticators can be lost, or taken over by an attacker. As smart card technology improves and a single common standard for their use emerges, organizations will have the option of combining two-factor authentication with physical access permissions on the same card.

The third way is to test something that is physically part of the user. This approach, commonly known as biometrics, uses fingerprints, voiceprints, and face or retinal scans. These systems are considered the ultimate in strong user authentication. However, high cost and intrusiveness mean that such systems are non-trivial to implement.

The most sensible approach is to combine two or more approaches, such as a password with an authenticator or biometrics. This approach, known as 'two-factor authentication', provides a much stronger level of security than any one approach on its own. It is therefore also known as 'strong' authentication.

User identification relates to the issuing and verification of appropriate access privileges to the authenticated person. Once an individual is authenticated, the user identification that is issued and the user privileges that are allocated to the individual are validated as the individual seeks access to various network resources. Access can be granted to some resources but not to others.

User registration and deregistration

Control 9.2.1 of ISO27002 says the organization should have a formal user registration and deregistration procedure that grants access to all multiuser information services and systems. Wherever possible, the organization should implement a single sign-on access management system, which ensures that a single user name and password enable a user to access all those assets he or she is allowed to access. A user access profile that contains a number of individual system and information access rights can simplify life for the user (there is only one set of information to remember and therefore fewer written records to compromise) and for the system administrator (it is easier to control and monitor access rights by an individual and to concentrate on tightening and improving security rather than administering multiple sign-ons). Single sign-on is available with Microsoft systems, and full details of related security issues are available from the Microsoft website. Microsoft Windows uses a security protocol called Kerberos to provide users with a single network log-on, which it does by using public key infrastructure to protect the information that is exchanged in the log-on process. Active Directory is a Microsoft directory service. An AD domain controller authenticates and authorizes all users and computers in a Windows domain.

ISO27002 recommends that an organization's user registration process should (reflecting on other controls as appropriate) cover the following:

1. Unique user identifications (IDs) should be issued so that users can be linked to, and made responsible for, their actions. The larger the organization, the more important it will be to have standard protocols that deal with separately identifying people who have the same name or whose user names might otherwise be the same. User names should not be easily guessed, although the larger the organization, the easier it will be for an attacker to find out through social engineering the structure of, and actual individual, user names. E-mail addresses (eg **john.doe@organizationname.com**) should identify users differently from the internally used user name (eg jsmith) that will enable the user to access system resources.
2. Group (shared) IDs should not be permitted except under exceptional, specifically approved situations where the business requires it. This is particularly important for the 'administrator' and, often, the 'guest' user names. Microsoft documentation (available from the Microsoft website) or system administrator manuals (available for each software

package, such as Windows 10, or SQL Server, or Server 2012, etc, in all good bookshops) set out how the system administrator user name should be dealt with (retired, and stored under appropriate physical security) and explain how to set up system administrators with individual user names. The ISMS should require all servers to be set up in accordance with the detailed security guidance contained in the relevant Microsoft security checklist, and this requirement should be included in the ISMS itself. Servers that carry sensitive information (such as financial information or substantial personal data subject to data protection legislation) should in addition be configured in line with any specific 'hardening' guidance available from CERT. There are also potential problems with 'guest' user names, and these should be properly understood and the appropriate steps taken to deal with them. The information security adviser should not simply accept the system administrator's statement that the servers are set up in accordance with best practice, but should obtain the documents identified here, determine what best practice actually is and ensure that the set-up conforms to it. Virtual servers should be subject to the same security approach.

3 The user's access rights should be documented and describe what assets and systems the user is allowed to access. System owners should authorize proposed users to use the system, and the access rights document should also be authorized by the individual's line manager, to ensure that it is appropriate. Effective security systems would also ensure that only those people identified as trusted employees of third parties or who have passed the employer's screening process are granted any access at all. Most usually, HR would originate the access rights document as soon as the background checks on a new employee are satisfactorily completed and should ensure that the requirements of the role as identified in the job description drive the proposed access rights.

4 The access rights granted should reflect the access policy in that they are in line with the policy's definitions as to who needs access to what. The policy should also not compromise on segregation of duties. This is particularly important in regard to access rights necessary for remote administration of a server or workstation network, as any user who has such access rights will be in a commanding position.

5 Ensure that the users get a written statement of their access rights. This can most simply be a copy of the document described in 3) above. Users should also be required to sign a copy of this, to signify that they

understand and accept their rights and that they understand that breach of them, and specifically any attempt to access services or assets that they are not authorized to access, may lead to disciplinary action and specific sanctions. This should also be linked to the organization's internet AUP and its e-mail policy, so that the access rights referred to in this document are also granted subject to the user agreeing to abide by both the internet and e-mail policies.

6 This user access statement should also refer explicitly to password management (control A.9.3.1), to specific privileges that have been granted (control A.9.2.3), to acceptable password structures (control A.9.3.1) and to the requirement for a password-protected screen saver and power off when not in use (control A.11.2.8). It should explicitly identify the services to which the user is authorized to have access (control A.9.1.2), should exclude the use of any software, of whatever provenance, for which the organization does not have a valid licence (control A.18.1.2) and should require the user to clear in advance with the organization's data controller the storage of any personal information (control A.18.1.4).

7 Ensure that service providers do not provide access until formal authorization processes are completed. It is better to complete this process before someone joins the company, and to do it as quickly as possible, as otherwise there will be pressure to give the person access to systems that might then be compromised.

8 A copy of the signed document should be placed on the employee's (or contractor's) individual HR file. The network administrator who is issuing the user name should also be able to access the central record so that he or she is at any time able to evidence that the listed user names on his or her system are all authorized.

9 The access rights of people who change jobs or leave the organization should be immediately removed. There should be an appropriate document that sets this out, which is triggered by HR, signed off by all the people concerned and used to authorize the removal of a user name. All of this is most important in situations when people are informed that they are to (or are about to) lose their job; it is not unknown for a disgruntled person at this point to take destructive action against the employer. The organization should draw up a clear policy on how it will handle the access rights of people who are to lose their jobs, in whatever circumstances, and implement it consistently.

10 Redundant user IDs should be removed; the user name register should be periodically checked against the current payroll and HR and third-party contractor files to ensure that only currently authorized individuals have user names. In organizations with even limited regular staff turnover, this check should probably be conducted every month, and an initialled copy of the checked user name register filed with the audit records.

11 Redundant user IDs should never be reissued. The person who used it might remember it and might want to attempt unauthorized access to the system; there would be no way of identifying that the attacker was an ex-employee and not the current member of staff.

User access provisioning

Control 9.2.2 of ISO27002 describes a formal process for the assignment or revocation of access rights. The idea here is that those who are allowed to access specific information or information services should be formally authorized to do so – both by the owner of the information asset in question and by management. This should link to the access control policy and the logic that the business should determine access rights. System administrators should retain a record (a log) of access rights granted and should, on a periodic basis, review allocated access rights to ensure they are still in with what has been authorized. The reality, of course, is that it is relatively common for an individual's access rights to need to change over time, in line with the changing day-to-day requirements of the business and of their role; however, these variations are seldom captured in the formal records, and the result is that there comes a time when no-one really knows what a given individual is able to access. This is not ideal.

It could, therefore, be a standard part of management checks or the internal audit programme to verify that User ID logs match actual access rights, that those whose roles have changed have had formal authorization for changes to their access rights, and that those who have left have had their access rights formally revoked.

Increasingly, Windows and various applications are providing the facility for organizations to set up user access roles, which contain standard access rights; this can significantly simplify the process of ensuring that any given individual has appropriate access rights.

Management of privileged access rights

Control 9.2.3 of ISO27002 says the organization should restrict and control the allocation and use of privileges in line with its access control policy. A privilege is any facility in a multi-user system that enables one user to override system or application controls. Inadequate control of privileges invariably leads to their inappropriate use; equally invariably, this abuse leads to system breaches and is a major contributory factor in system failures. The most critical privileges are those that enable system administrators to do their jobs.

The organization should develop, in its ISMS, rules for the allocation of privileges that start by identifying, for each system (operating system, application, database, etc), the privileges associated with it and the categories of staff to whom these privileges might need to be allocated. Privileges are usually identified in terms of user categories (eg system administrators) and users are allocated privileges by being joined to user groups that have specific privileges. The product manuals for each application contain this information. Users who might need these privileges should, in the first instance, have user names for everyday use that have virtually no privileges assigned to them. Privileges should be assigned to a separate user name so that it is harder for an attacker to view its use and harder for a user to exercise one of the privileges inadvertently.

Privileges should be allocated on a 'need-to-use' basis and, where possible, event by event, so that users have only the minimum requirement for their functional role, and only for as long as needed. There should be an authorization process for the allocation of privileges (which should be available through a separate User ID), which should be part of the documented user authorization process referred to above. The user should not be allowed any special privileges until authorization has been formally granted. Managers should be aware that many staff, particularly technical staff, get an increased sense of self-importance out of having privileges in excess of those needed for their jobs and will browbeat managers (and try a number of other tactics) in order to get them. These attempts must be resisted; an allocation system that requires privilege allocation to be decided by someone other than a user's direct line manager is therefore an effective control against inappropriate privilege allocation.

Finally, it not only makes sense to ensure that those to whom privileges are being given are actually competent to use them (remember the Standard's requirements in relation to competence), but there should also be a specific

process for removing privileged rights when they are no longer needed. Most importantly, when a system administrator or someone who has had such privileges leaves the organization there should be an immediate review of privileged User IDs and passwords.

Management of secret authentication information

Control 9.2.4 of ISO27002 says the organization should control allocation of secret authentication information through a formal and managed process. Passwords are a commonly used type of secret authentication information, commonly used to verify a user's identity. Other types of secret authentication information include PIN numbers, cryptographic keys, data stored on hardware tokens (eg smart cards) that produce authentication codes and, potentially, biometric information. While the ISMS requires specific behaviours of users (described in control 9.3.1), this control is to do with the organization's side of authentication management and recognizes that the easiest method of malicious access to an organization's network is through nefarious password acquisition:

1. Users should accept in writing that they will keep passwords and other authentication information confidential and will use any group passwords only in accordance with the rules attached to them; this statement should form part of the user access statement identified in relation to A.9.2.1.
2. Where users are required to choose and maintain their own passwords, they should be issued initially with a secure temporary password, which they are forced to change immediately on first log-on. When users are issued temporary passwords after they forget their own passwords, this should only be done after the user has been positively identified, preferably face to face. This is to stop someone who has obtained a valid user name from also obtaining unauthorized access to the system simply by claiming to have forgotten his or her password (a form of social engineering).
3. Temporary passwords should be unique to an individual and not guessable, and should be delivered securely to users; they should not be sent in clear across the internet or via non-trusted third parties. Some form of secure delivery protocol should be used. Users should acknowledge receipt of passwords in writing.

4 The helpdesk function that deals with lost or failed passwords needs effective management, careful training and audit to ensure that any attack on the system by this route can be controlled.

5 Passwords and other authentication information should never be stored in or on computer systems in clear view – the yellow sticky note on the computer screen is the classic aid to unauthorized access – and should never, ever, be stored in system files or on websites in anything other than encrypted form. Default vendor passwords on every single item of computing hardware or software should be changed on installation. There should be an audit process to ensure that these passwords have been changed.

Review of user access rights

Control A.9.2.5 requires the ISMS to contain a formal procedure for the regular review of user access rights, so that effective control over access to data and information services is maintained. Principles of the review procedure might include:

- Review of normal access rights on a predetermined regular basis; ISO27002 recommends every six months, or after any changes in the system, structure or the individual's role.
- Review of privileged access rights on a predetermined but more frequent basis; experience teaches that every three months is the interval which best combines security with memory.
- Privilege allocations to be checked at regular intervals – perhaps monthly – to ensure that users have not obtained unauthorized privileges, usually through collusion. Any instances where someone has obtained unauthorized privileges should be thoroughly investigated and disciplinary action considered.

This review can be carried out by the information security adviser in conjunction with the line managers of the individuals concerned, and the outcome of the review should be documented – most simply by an annotation on all the copies of the original privilege allocation document – and reported en masse at the subsequent meeting of the information security management forum for formal approval.

Control A.9.2.6, covering removal or adjustment of access rights, was covered in Chapter 8, along with the other controls that deal with termination of employment; these apply to end-of-project or role change scenarios.

Use of secret authentication information

Control A.9.3.1 recognizes that the cooperation of users is essential for effective information security and requires the organization to ensure that its users follow good security practices in the selection and use of passwords and other authentication techniques. This is best done by taking two steps. The first is to set out, within the ISMS, a clear set of rules about password selection and use, which are then incorporated into the user access document (as a separate section), which the user signs to signify agreement. The second is to set up the system software in such a way that it enforces key components of these rules (control A.9.4.3). The password use rules should require users:

- To keep passwords confidential, which includes in no circumstances giving them to a third party, whatever the ostensible reason.
- To avoid keeping any paper or electronic record of passwords (unless this can be securely stored – which means encryption and strong, two-factor access control protection).
- To change a password whenever there is any possibility that it may have been compromised. This means that password management software should not be configured to prevent users from changing their password, because if they have to 'report' their stupidity in compromising their password to a service or helpdesk, they might not do so and could continue to use a compromised password.
- To select passwords that have a minimum length of seven characters (eight might be better, assuming users will be able to recall their password without writing it down), and this requirement can be set in the system software. These passwords should not be based on anything easy to guess such as dates of birth, names, telephone numbers or other person-related information, should not contain words that occur in dictionaries (because these would be vulnerable to automated dictionary attacks) and should not contain consecutive identical characters or all-numeric or all-alphabetical groups. Many dictionary attacks now include replacing obvious alphabet characters with numerals such as l with 1, o with 0 and e with 3 and even special characters such as a with @.

- To change passwords regularly. The system software can be set to enforce changes, say every 90 days, with a defined pre-change period during which a warning of the impending requirement is flagged so that someone who will be out of the office at the point that the change is enforced can change the password in advance. The system can also be set so that passwords cannot be recycled, and this should be done so that the user is forced always to have new ones. Sequential passwords (so Jamaica 1, Jamaica 2, etc) should not be possible.
- To change temporary passwords at first log-on.
- Not to store passwords in any automated log-on process, unless expressly so permitted.
- Not to share passwords under any conditions – and this includes not using the same password for business and private affairs.

One technique for creating strong passwords is to use a pass phrase. For example, if you were to use 'I eat three Shredded Wheat at breakfast time' as a pass phrase, you would select the first character of each word (and perhaps replace some of them with special characters or different cases) to give a password such as Ie3SW@bt.

It is important to bear in mind that the proliferation of differing strong password policies, across multiple sites and vendors, combined with the need for frequent changes, can create challenges for many individuals in meeting all of the above requirements. Increasingly, organizations have to consider Single Sign On options, and have to be prepared to allow the storage of passwords in password vaults on smartphones. Such a step will create significant risks, but it may be easier to manage those risks than to continue coping with the complexities of the current range of authentication requirements.

13

System and application access control

The overall control objective for this group of controls is to prevent unauthorized access to systems and applications.

Information access restriction

Control A.9.4.1 requires the organization to restrict access to information and application system functions in accordance with the access control policy that was specified in control A.9.1.1. The business owner of an application (and any related data) must define who will have access to that application and, in terms of any data within it, at what level (ie read, write, delete, execute). Users should be given only the minimum level of access that they need to an application or its data, as access to too much can increase the risk of breach of confidentiality and/or loss of integrity. In financial applications, over-authorization can lead to the possibility of fraud. It is particularly important to define access levels in respect of shared data-bases; each group of users should be able to access only data that are relevant to those users' own business or activity.

Additional measures that should be considered are:

- Providing access menus on user screens that control (by their limitations) access to application systems and their functions. This control is implemented by the system administrator and can be done most simply by providing 'standard builds' for desktop software that precisely reflect the business use needs of a specific group of users, and changes to which can only be made by the system administrator on receipt of appropriate authorization.

- Not training in the use of, or restricting knowledge of, application systems and functions that are not required, and editing system documentation or work instructions to support this process.
- Limiting provision of access rights to individuals so that even if they are able to bypass the system menus, they are unable to access applications that the business does not need them to access.
- Controlling the access rights of individuals such that they can carry out only the functions they need to, such as read, write, delete or execute, recognizing that for many applications, individuals only need read access and that the best way of preventing someone from carrying out unauthorized deletion or amendment of information is to make it impossible for him or her to do it.
- Ensuring that application system outputs (from systems handling sensitive data, as defined in the organization's information classification system) are sent only to authorized terminals or locations and that these outputs are periodically reviewed to ensure that redundant information is removed. Some sensitive systems should be considered for isolation, either physically or logically, to limit their exposure to significant risks.

Secure log-on procedures

Control 9.4.2 of ISO27002 says the organization should use a secure logon process in providing access to information services. This should be considered alongside control A.9.2.4, Management of secret authentication information, and A.9.3.1, Use of secret authentication information. A secure log-on process is one that discloses the minimum of information about the system in order to avoid giving an unauthorized user any assistance. It should be designed to minimize the opportunity for unauthorized access to the system, remembering that poor password control is one of the easiest methods for attackers to gain access. The procedure should, as a minimum, be configured by the system administrator using the set-up options provided within the Microsoft package and reflecting the risk assessment:

- The screen should display no system or application identifiers until the log-on has been successfully completed.
- The display on the log-on screen should include a general notice warning that the computer should be accessed only by authorized users. with a

brief description of the criteria by which they are identified (eg employees of organization X).

- The screen should not provide help messages during the log-on procedure (particularly not warnings about how many incorrect entries are allowed).
- The system should validate the log-on data only on completion of input and then, if there is an error, the system should not explain which part of the data is incorrect but simply require the user to try again.
- The log-on procedure should limit the number of unsuccessful attempts allowed to three (and unsuccessful attempts should automatically be recorded), and automatically either enforce a time delay before further attempts are allowed or simultaneously disconnect the data link, send an alarm and reject any further attempts without specific authorization from the system administrator, the user having first been positively identified by the system administrator.
- The system should limit the maximum time allowed for the log-on attempt, and when the limit is exceeded, the system should terminate log-on; authorized users can correct log-on errors quickly, whereas attackers might need more time to guess the correct details.
- The screen should display, after a successful log-on, details of the date and time of the previous successful log-on (so that an authorized user can see whether the previous log-on was someone else or not) and details of any unsuccessful log-on attempts (so that the user can immediately report this as a security incident).
- Finally, the password characters should be hidden by symbols and always encrypted before being sent across the network.

Two other controls that might be considered, depending on the risk assessment, would be the automatic termination of inactive sessions after a pre-determined period, and a restriction on connection times – both of these particularly useful for mobile devices and nodes outside the secure perimeter.

Password management system

Control 9.4.3 of ISO27002 says the organization should have an interactive password management system that ensures quality passwords. Again, this clause should be read in conjunction with control A.9.3.1 for situations in which passwords are chosen by the users. A good system will enforce the use

of individual passwords and will allow users to select and change their own passwords, including a confirmation procedure to flush out any errors. The selection of password characters of a minimum length should be enforced, as should regular password changes.

In addition, the system should maintain a record of previous passwords and not allow them to be repeated for a defined period (eg for 12 months, or for ever), should not display passwords on the screen while they are being entered, should store passwords in an encrypted form using a one-way algorithm and separately from application system data, and should certainly alter default vendor passwords immediately following installation of software and hardware of any description. No user names should be permitted to operate without passwords.

Users must have the facility to alter their password at any time that they feel that its confidentiality has been breached. Some organizations do not allow this in their 'default' user configuration as they have experience of users changing their passwords x + 1 times (where x is the number of passwords checked for repeats and sequences by the system) in a matter of minutes, so as to enable them effectively to retain the same password. Either option presents a pitfall. The pitfall with the first option is as described above. The pitfall with the second is that forcing users to contact an administrator to change their password in advance of the regular, system-enforced change creates an additional obstacle to the process and could lead users to hope that nothing will come of the potential security incident and leave them, therefore, more likely to ignore it than to own up and create more work for themselves and others.

Use of privileged utility programs

Control 9.4.4 of ISO27002 says the organization should restrict and tightly control the use of system utilities. System utilities, which are there to help system administrators, might be capable of overriding system and application controls. Their use must therefore be restricted. The information security adviser and the network system administrators should first identify all the system utilities available and the security risks associated with them. The restrictions that ISO27002 recommends might be applied, to some or all of the utilities (and, again, a risk assessment will help make appropriate judgements here), are:

- identification, authentication and authorization procedures for system utilities;
- segregation of system utilities from applications software, and not making system utilities available to users who have access to applications where segregation of duties is required;
- limitation of their use to a small number of trusted users;
- ad hoc authorization for system utility use in specific circumstances and/or for a pre-specified period;
- logging and monitoring of all use of system utilities;
- removal from the system or disabling of all unnecessary utilities.

Access control to program source code

Control A.9.4.5 of ISO27002 says the organization should maintain a strict control over access to program source code and associated items, usually kept in program source libraries. ISO27002 sets out very clearly the steps that an organization ought to take to protect its program source library. It is not directly relevant to an environment that runs only COTS or pre-packaged software, and therefore is not discussed further here. The statement of applicability (SoA) can afford to make this or a similar comment against this control in the documentation.

Where program source codes and associated items do exist, access to them should be controlled in line with ISO27002, 9.4.5.

14

Cryptography

ISO27002 says, at 10.1.1, that the organization should develop and follow a policy on the use of cryptographic controls for the protection of information.

Any decision as to whether or not a cryptographic solution is appropriate should be part of the wider process of assessing risks and selecting controls. A risk assessment should determine the necessary level of protection to be given to information, and a cost–benefit exercise should be carried out. This risk assessment should also address issues such as unauthorized circulation of encryption keys; it might be appropriate for the organization to retain copies of all employee encryption keys against the danger of their being lost or of a disgruntled employee first encrypting critical information and then destroying the key or removing it and holding the organization to ransom.

If the risk assessment indicates that cryptographic controls are appropriate, the organization needs to develop a policy statement within its ISMS that sets out how it intends to deal with this issue. The basic principles that the organization is going to apply need to be implemented across the whole organization. The policy statement should include a description of the management approach and general principles under which information should be protected. These should include the following:

- The circumstances under which business information should be protected, why this might be necessary (ie the risks that are being addressed) in relation to the sensitivity of particular types of information and the means by which they are being transported (whether wireless, mobile device, removable media, etc), and how the appropriate level of cryptographic protection is determined (assuming that the individual operator has any discretion in the issue) should all be identified.
- The required level of protection (and this should be reflected through a documented risk assessment) should be assessed, taking into account the

type, strength and quality of the encryption algorithm that is being deployed.

- How encryption keys should be managed and how to deal with lost, compromised or damaged keys, responsibilities, standards, etc should be specified.
- Roles and responsibilities in regard to implementation of the policy, and the generating and management of keys, should be set out.
- Where more than one cryptographic standard is to be deployed, the policy should identify which standard applies to which process and information classification so that there is no room for error or uncertainty.
- The policy should be communicated to all users before any use of these controls commences.
- Consideration must be given to any legislation or regulation that may cover the use of encryption. In the United Kingdom, for instance, use of cryptography and digital signatures is subject to the Electronic Communications Act 2000.
- It is possible that the organization's policy may be to not allow encryption; such a policy should still be documented.

Encryption

Encryption enables the organization to protect the confidentiality of sensitive or critical information. There are two types of encryption: symmetric encryption, which uses the same key (or code) to encrypt and decrypt data; and asymmetric encryption, which uses one key to encrypt information and a completely different (but mathematically related) key to decrypt it.

Symmetric encryption

Data Encryption Standard (DES) is a widely used symmetric encryption standard. It is used for long communications and is relatively speedy to use. It is, however, quite an old system and this has led to triple DES, in which the same data are encrypted three times, employing different keys, which exponentially increases the strength of the encryption. Only the creator and receiver have the DES key (or keys); the key(s) are usually exchanged using either a shared master key or a pre-existing key exchange protocol.

Asymmetric, or public key, encryption

Under this methodology, an organization has two keys, one private and one public. Anyone can use the public key to encrypt a message for the organization, knowing that only the possessor of the private key will be able to decrypt it. Equally, anything that decrypts properly using the public key must have been encrypted using the complementary private key. A critical issue in public key cryptography is to attest the validity of the key pair and, in particular, that the named public key really is the organization's public key. This is done with a digital certificate (sometimes called a server ID but more correctly a Subject Key Identifier, SKI).

A digital certificate is an encrypted file that attests to the authenticity of the owner; it is created by a trusted third party known as a certificate authority (CA). A CA will review the credentials of any organization that wants a digital certificate before issuing it. This review will include the Dun & Bradstreet number or Articles of Incorporation and a thorough background check to ensure that the organization is what it claims to be. Applications can usually be done online, via the CA's website, and the verification process will typically take between one and three days.

The digital certificate is proven to be authentic because it contains the CA's distinguished name and decrypts correctly using the public key of the CA. The CA may be a secure server on the network (the single trust model) or an external organization recognized by many (the multi-party trust model). The keys used are either 40-bit, 128-bit or 256-bit.

Public key infrastructure

Vendors of public key technology have been working to create an industry-standard implementation that standardizes certificate types as well as the principles used for recognizing and managing a CA, the trusted party that issues certificates to identified and known third parties. Critical issues in the development of public key infrastructure (PKI) include directory services for locating certificates for particular individuals, and means of effectively communicating revocation of certificates, particularly when an organization ceases to trade and its certificate and technology are acquired by a less scrupulous operator than the one that originally obtained the certificate. X.509 is the current standard for PKI; it defines standard formats for certificates and a certificate validation algorithm.

The organization should, again, use a risk assessment to determine whether or not encryption is a key component of its ISMS. The two main areas for which encryption should be considered are the protection of sensitive information on notebook computers and the protection of information being sent across public networks. Only the most sensitive of information (depending on its classification) travelling on public networks should need to be encrypted, and such a policy should be adopted only if all components of it can be fully implemented. Dangers include employees losing keys (which would render useless, and potentially irretrievable, anything encrypted with them).

If the outcome of the risk assessment is that encryption is an appropriate protection, then specialist advice should be sought in selecting an appropriate technology and in considering any legal implications that there might be in using encryption, or cryptographic technology. Most large, specialist security organizations could provide specialist advice on cryptography. This advice should reflect the latest situation in terms of government restrictions (in the United Kingdom, the Electronic Communications Act 2000) on the use of cryptographic technology and the countries in which it can and cannot be used.

Digital signatures

Digital signatures can be applied to protect the authenticity and integrity of electronic information. Digital signatures can be applied to any form of electronic document, such as electronic payments, funds transfers, contracts and agreements. Symmetric cryptography systems do not support the enhanced proof of data integrity that is required for a digital signature. The public key methodology is ideal for this; a digital signature is used to assure both sender and receiver that a sensitive document originated as represented and that it has not been tampered with since origination.

This is done by using a one-way hash function to transform a document into a unique, fixed-length character string (or digest), which is included with the transmitted and encrypted document. Any changes that are made to the original document will change the digest, and when the receiver runs the hash function on the received file, it will not duplicate the digest. Digital signatures are thus strong proof that a file is genuine and in its original form, and therefore digital signatures have a role to play in non-repudiation.

However, organizations should also take legal advice on the status of digital signatures within the jurisdiction that they will want to uphold the underlying agreement. Not all countries have the same level of recognition of digital signatures, and therefore additional agreements between organizations may be necessary, setting out clearly the basis on which they will use and recognize digital signatures. This means that organizations should consider the cost–benefit equation in respect of using digital signatures and should not embark on this course lightly.

Clearly, the confidentiality of the private key has to be protected, and the organization needs to address this specifically so that it can ensure that only authorized personnel have access to it and that records of its use are maintained. The public key should logically be protected by using one of the recognized certificate authorities.

Non-repudiation services

Non-repudiation services can resolve disputes about the occurrence or the non-occurrence of an event or action. While someone could, for instance, copy an e-mail to himself or herself or retain a copy in his or her outbox, to provide some proof of both origin and dispatch, this is not foolproof. A proof-of-receipt e-mail (which can be set up in the sending person's instance of Outlook) from the receiver's e-mail server is also not ironclad.

The discussion, above, of public key infrastructure dealt with the services offered by CAs. Such trusted organizations can provide evidence of origin, submission and receipt that are ironclad. They do this by applying digital certificates to e-documents. Proof of origin, for instance, is provided by the CA attaching its digital signature, encrypted with its private key, to the communication that is to be authenticated, and this attests to the authenticity of both the document and its creator. Proof of receipt is provided by a digitally signed document sent via the CA stating that it has been received.

Once the organization has chosen and been accepted by a CA, there should be a contract in place with the CA that specifies the service to be provided, all in accordance with the ISMS requirements. These contracts should cover issues of liability, reliability of services and response times for the provision of services.

Electronic document signature services, usually offered on a SaaS basis, can provide very inexpensive mechanisms for sharing digital signatures in a

non-repudiation environment, provided both parties formally accept digital signatures.

Key management

Control 10.1.2 of ISO27002 says the organization should set out, in its ISMS, an encryption key management system that is based on an agreed set of standards, procedures and methods that support the use of cryptographic techniques. As ISO27002 points out, any compromise or loss of a cryptographic key can lead to compromise of confidentiality, integrity or availability of information. Clearly, therefore, the organization needs to put in place a management system that reflects the risk assessment and is appropriate for the cryptographic technique that it uses. There are, as explained above, two types of encryption, and the organization may use one or both of them.

A symmetric encryption technique will require the organization to keep secret its key, as anyone who obtains the key will be able to decrypt any information encrypted with it. The private key for an asymmetric system must also be kept secret, for the same reason, although the public key is obviously intended to be accessed by the public. All keys, both secret and public, should be protected against unauthorized modification or destruction. Physical protection should be considered for any equipment used to generate or store cryptographic keys.

The ISMS should set out how these keys are to be managed. Technical input into this section of the ISMS should be provided by the information security adviser or the supplier of the cryptographic tools selected by the organization. ISO27002 sets out a number of issues that it recommends should be considered for inclusion in a procedure for private or secret key management. The questions that should be answered as part of a risk assessment process are as follows:

- How are keys to be generated for different cryptographic systems and different applications?
- How are public key certificates to be generated and obtained?
- How should keys be distributed to intended users and how should they be activated?
- How should keys be stored and how should authorized users access them?

- How should keys be changed or updated and when? (For preference, keys should have defined activation and deactivation dates so that the risk of compromise is reduced.)
- How should compromised keys be handled?
- How should keys be revoked, withdrawn or deactivated and when? (For example, when a key user leaves the organization.)
- How should keys that have been lost or corrupted be recovered (so that encrypted information can be retrieved)?
- How should keys be archived (because information encrypted with them may later need to be decrypted with them)?
- How should keys be destroyed, if at all, and when and on what authorization?
- How should key-related activity be logged, monitored and audited?
- How should legal requests for access to cryptographically encoded material be handled? (The unencrypted version of currently encrypted information might, for instance, be required as evidence in a court case!)

Public keys also have to be protected. Unless a public key certificate is used, there is always the danger that someone might forge a digital signature by replacing an organization's public key. The only really reliable way to produce such a public key certificate is to use a recognized certification authority.

15

Physical and environmental security

Control category A.11 deals with physical and environmental security. It deals with what might be called geographic or area security, with equipment security and with general controls to protect physical assets. Large or multi-site organizations might, as discussed in Chapters 5 and 6, need to break themselves down into a number of physical domains (giving due consideration to any communication links between them) and then consider each domain on its merits.

Secure areas

Control objective A11.1 deals with secure areas. Its objective is to prevent unauthorized physical access, damage or interference to business premises and information. It has six sub-clauses. Critical or sensitive information and information processing facilities should be housed in secure areas protected by a defined secure perimeter, with appropriate security barriers (eg walls, fixed floors and ceilings, card-controlled entry gates) and controls (eg staffed reception desks) that provide protection against unauthorized access or damage to papers, media or information processing facilities. The protection implemented should be commensurate with the assessed risks and the classification of the information, and should take into account out-of-hours working and similar issues.

Physical security perimeter

Control 11.1.1 of ISO27002 says the organization should use a security perimeter to protect areas that contain information processing facilities. It may be appropriate, depending on the risk assessment and the classification

of the information being protected, for an organization to use more than one physical barrier, as each additional barrier may increase the total protection provided.

The first step is to use a site or floor plan to identify the area that needs to be secured. A copy of this document should be found with the property title deeds. The plan that is with the deeds is there to show clearly the premises that the organization owns or leases, and it is the most appropriate base document to use for defining the secure perimeter as it identifies clearly the property over which the organization has control.

A continuous line should be drawn around the premises on the site plan, including all the information and information processing facilities that need to be protected. This line should follow the existing physical perimeter (and a perimeter in this context is something that provides a physical barrier to entrance) between the organization and the outside world: walls, doors, windows, gates, floors, fixed ceilings (false ceilings hide a multitude of threats), skylights, etc. Special attention should also be given to lifts and lift shafts, risers, maintenance and access shafts, etc. This site plan, showing the defined physical perimeter, should form part of the ISMS records. The ISO27001 auditor will almost certainly want to see it and then to test the effectiveness of the perimeter.

A comprehensive risk assessment should be carried out to identify the weaknesses, vulnerabilities or gaps in this perimeter, and from this assessment the appropriate physical controls – the additional physical barriers, such as doors, card-controlled gates, staffed reception desk, etc – can begin to be identified. While not all organizations will have information as valuable as that obtained by Tom Cruise's character, Ethan Hunt, in the first *Mission Impossible*, the way in which he gained access to the room within which it was kept indicated that the guarding organization's risk assessment had not been sufficiently thorough. There was a vulnerability in the physical perimeter that Ethan Hunt identified and then exploited in a way that demonstrates that 'difficult to imagine someone coming in through those ducts' was an inadequate approach to securing the physical perimeter. The ISO27001 auditor should want to see the documented risk assessment and will analyse its thoroughness and effectiveness, initially by challenging the person responsible for defining it and then, after inspecting likely vulnerable areas, by probing to see how secure it actually is.

The following controls should form part of the implemented security perimeter:

- The perimeter itself is defined (and the secure environment within it is an asset that should have been the subject of a risk assessment) in a document and, if possible, by means of appropriate signage, and staff are aware of what and where it is.
- The perimeter (particularly of a building containing information processing facilities) should be physically sound. There should be no gaps in the perimeter (risers, lift shafts, air-conditioning vents, etc should all be assessed) or areas where a break-in could easily occur. The external walls should be of solid construction and all external doors should be protected against unauthorized access using appropriate control mechanisms, one-way bars, alarms, locks, etc.
- There should be a staffed reception area or other means to control physical access to the site or building. Access to secured premises should be restricted to authorized personnel only.
- Physical barriers should be extended from real floor to real ceiling (ie below and above any false floor or false ceiling, particularly those installed to provide effective ducting for cabling) to prevent unauthorized entry or environmental contamination such as that caused by fire or flood.
- All fire doors on a security perimeter should open outwards only, should slam shut (because they have working door-closing mechanisms fitted to them) and should be alarmed (and this fact should be advertised on the doors to try to prevent inadvertent false alarms). Some organizations site CCTV cameras to cover these doors to watch for deliberate false alarms that might be designed to distract security staff attention from a planned point of real break-in elsewhere or to enable a perimeter breach before security staff can attend.
- Appropriate intruder detection systems (which are manufactured to relevant standards) should be professionally installed and maintained. All external doors and accessible windows (particularly on the ground floor) should be covered, and unoccupied areas should probably be alarmed. The alarm cover should be specifically extended to include computer and communications rooms. Copies of test certificates, schedules of key holders and alarm response procedures (who is to do what when an alarm goes, including out of hours) should be retained as part of the ISMS records. Key holders should receive training in how to respond to alarms, what to do to secure the site after a break-in or other incident,

and what the escalation procedure is. The alarm response procedure should be reviewed after every alarm incident, and where a police response service is part of the security set-up, every effort has to be made to avoid false alarms, as these can lead the police to withdraw their cover. This is particularly important where the organization includes a manual alarm trigger at, for instance, the reception desk to help deal with unwanted intruders during opening hours; these alarms can easily be triggered accidentally. However, making them awkward to trigger detracts from their effectiveness in addressing the reason for having them in the first place.

There are particular problems where two or more organizations share physical premises. In these circumstances, more than one secure perimeter may be necessary. For instance, there may be a staffed reception desk that lets employees of both organizations on to the property according to jointly agreed procedures. Each organization might then restrict access to its own floors, either through key cards or through its own reception desk. Where this type of additional perimeter is not possible, there may need to be individual security perimeters around individual information assets or information processing facilities in order to ensure that the organization's information processing facilities are physically separated from those managed by any third parties.

Physical entry controls

Control 11.1.2 of ISO27002 says that secure areas (see A.11.1.3, which is discussed below) should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access to the premises. ISO27002 recommends specific controls, some of which are more difficult for smaller companies, but which are nevertheless worth considering and, wherever possible, implementing:

- Visitors to secure areas – whether the site itself or specific areas within the site – should be supervised, or cleared in advance, and their date and time of arrival and departure recorded. Access should only be granted for specific, authorized purposes and all such visitors should be issued with instructions on the security requirements of the area and on emergency evacuation procedures. These instructions are usually recorded on a standard visitor's pass, which itself records the date and time of arrival into a ledger on which the departure details can be recorded when the

visitor leaves. Good practice would usually require the security staff issuing the visitor's pass to confirm by telephone that the visitor is expected and the purpose of the visit. A more secure set-up would be for the visitor's details to be notified to the reception desk in advance and for a telephone check to take place when the visitor arrives. In high-security areas, these visitor lists might have to be approved by a senior line manager before they are forwarded to the security desk. Visitors should be accompanied everywhere by a member of staff, and where necessary their identity should be reconfirmed prior to access to other sections of the secure area being granted. Visitors' passes should use some slightly complex and visible system of demonstrating whether or not they are still valid; for instance, all passes issued on a Monday might have a black dot, those issued on Tuesdays a red square, etc.

- The selection of security services is itself a security risk. Not all such companies take appropriate steps to vet and train their operatives, and it is therefore essential that appropriate controls in respect of external parties are fully implemented. No matter what their prior training or experience, security guards should also receive training in the internal security procedures of the organization for which they are providing security services.
- Where access for unauthorized people to the site or building is controlled remotely from the reception desk, there should be an effective communication tool that enables the receptionist to identify (both verbally and visually) the visitor before allowing access.
- Access to sensitive information, and information processing facilities, should be controlled and restricted to specifically authorized persons only. This is particularly important for the computer server room(s), access to which needs to be severely limited. Authentication controls, such as a swipe card and/or individual PIN codes, should be used to authorize and validate access to secure areas, and to secure areas within the security perimeter. If possible (and if required by the risk assessment), the swipe card entry system should also provide an auditable trail of access. The record of visitor passes issued should be maintained in a secure location, as it might, at some point in the future, be required to identify an intruder.
- All personnel should be required to wear some form of visible identification (which could be incorporated with an access card – which might work through swiping, physical proximity or biometric accuracy) and

should be encouraged to challenge or report unescorted strangers or anyone not wearing visible identification. A visible identification badge is a control far more important in a large organization than in a small one, but in any size of organization, unidentified and unaccompanied visitors should always be challenged. There are many organizations for which this, on its own, will require a significant culture change, and this could significantly contribute to improved security. Of course, even in a small organization the fact that visitors have to wear badges acts as a deterrent to opportunist trespassers or intruders, as they will realize that they are obviously out of place without the appropriate visual 'stamp' of approval (assuming this control is implemented effectively and passes are retrieved from visitors and staff leavers who no longer have need for them).

- All staff who might encounter visitors should be trained so that it is difficult for a social engineer to bypass physical security controls.
- Access rights to secure areas should regularly be reviewed, updated and, where necessary, revoked. This is particularly important for access rights to computer server rooms. The record should be reviewed on a regular basis by the information security management forum, and a record of the forum's review should form part of the ISMS documentation.
- Third-party support personnel should have access rights that are, to the greatest extent possible, restricted to those secure areas or information processing facilities they need to access for specific times, and these access rights should be monitored, reviewed and, where necessary, revoked.

Securing offices, rooms and facilities

Control A.11.1.3 requires the organization to create secure areas within the security perimeter to protect offices, rooms and facilities that have additional, special security requirements. A secure room may contain lockable cabinets or safes. Secure rooms could be any rooms within the premises but will certainly include server rooms, telecommunications rooms and plant (power and air-conditioning) rooms. Some other areas (such as accounts or HR, or directors' offices) might also need to be secured. Many CEOs' offices should also be treated as secure rooms.

There could be a clash, within organizations that are strongly committed to open-plan working, between the desire for openness and the need for security. This will have to be addressed and solutions found that can be consistently and coherently applied across the whole organization. Part of

the solution will lie in what sort of meeting rooms or available secured areas can be used by employees, and part will depend on how information is classified and what facilities are made available for its storage.

ISO27002 provides very common-sense advice on the selection and design of a secure area, and this section should be read in conjunction with the next sub-section, 'Protecting against external and environmental threats'. Secure area design should take account of the possibility of damage from fire, flood, explosion, civil unrest and other forms of natural or human-created disaster. The risks posed by neighbouring premises should be considered, such as potential leakage of water from outside the secure area. Secure storage facilities, such as safes and high-security document stores, also need to be sited in such a way that they can be located on a site map within the business continuity documentation and quickly and easily recovered after a disaster. This will require consideration to be given to issues such as the fire-resistance period of surrounding doors and floors; the organization wants to avoid scenarios where, for example, after an explosion in the building, a safe containing all the organization's insurance documents falls from its location on the first floor right through into the basement of the building and has to be recovered (when it can be found) from among the debris of fire and flood.

The controls that ISO27002 recommends should be considered and, if appropriate, implemented include the following:

- Key storage areas and keyed entrance areas should be sited to avoid access by unauthorized persons and by the public.
- Buildings that contain information processing facilities should be unobtrusive and give as little indication as possible of their presence or purpose.
- Office machinery, such as printers and photocopiers, should be sited within the secure perimeter in such a way that access to more secure rooms is not required. In other words, do not put the scanner or printer machine in the same room as the computer servers, nor in a public area where unauthorized individuals may access the output.
- Doors and windows should be locked when the building or room is unattended. External protection, such as burglar bars, should be considered in the context of the risk assessment for ground-floor and any other accessible windows. This is particularly important for the computer server and communications rooms, which should be accessible only to a small number of authorized personnel, each of whom has individual access codes so that a record of access and egress can be maintained at an indi-

vidual level. No one should be allowed into one of these rooms unless accompanied at all times by an authorized person. Externally, any special precautions taken for specific rooms (eg whitewashed windows or bars) should not stand out in comparison to other rooms, as this would clearly indicate to a potential intruder where the most valuable assets might be stored. There should be no obvious signs outside the building to indicate how valuable or important a room is.

- As discussed earlier, information processing facilities managed by the organization should be physically separate from those managed by third parties, even if this means erecting a cage or some other form of physical security within a shared secure area.
- Internal directories or telephone books or other guides that identify the location or telephone numbers of secure, sensitive areas should not be accessible by the public or unauthorized persons.
- Hazardous or combustible material, particularly office stationery, should not be bulk-stored within a secure area. There should be a separate area, some distance away, where such material is stored. Regular inspections of secure rooms, by someone other than those responsible for their day-to-day management, are usually necessary to ensure that this requirement is observed.
- Back-up equipment and media should not be stored with the equipment that they will back up, in order to ensure that the organization can actually restore operations if it loses or otherwise has compromised its front-line facilities (through, for example, fire in the server room or terrorist activity affecting the whole of the premises).

Finally, a word about keys: keys should not be left in locks, irrespective of whether or not the access route has an automatic door closer. If the lock has not been engaged, it is possible for the key to be used by someone (whether accidentally or maliciously) to activate the lock, thus restricting planned access or egress at a later time.

Protecting against external and environmental threats

Control 11.1.4 of ISO27002 encourages organizations to protect themselves from damage due to fire, flood, earthquake, explosion, civil unrest and other forms of natural or human-created disaster. The discussion, above, about external threats to secure areas should be applied to the organization's general physical locations. In a sense, this control is asking the

organization to ensure that it has complied with health and safety and fire regulations and that it has carried out all the relevant risk assessments required by these regulations, while the comments, above, about controls against threats to secure areas apply more generally. In particular, there should be an appropriate site-level risk assessment covering the possibility of all these natural or human-created disasters; premises in a known earthquake area, for instance, face a greater threat than those elsewhere, and the organization's business continuity plan will need to take appropriate account of the threat. Similarly, likely local activity (including that of neighbours) should be considered, as should the risks of particularly high-profile locations – for instance, there might be protest marches, terrorist atrocities or police activity near government offices. In particular, choice of fall-back locations should be driven by consideration of likely repercussions of particular events: the diameter of the area likely to be affected by a bomb explosion, the likely effect of a police cordon, etc.

The auditor will want to see, and the board will want to know, that an appropriate risk assessment has taken place and that appropriate controls against such disasters have been implemented. Of course, these controls must be consistent with the corporate risk treatment plan.

Working in secure areas

Control 11.1.5 of ISO27002 says the organization should implement controls and guidelines for working in secure areas, to enhance the security provided by being within a secure perimeter and/or a secure area. These additional controls are largely common-sense extensions of the controls discussed earlier. ISO27002 suggests that the organization consider the following additional controls:

- Only allow employees (or contractors or third parties) to know about the existence of, or activities within, a secure area on a 'need-to-know' basis.
- Avoid unsupervised working within secure areas so as to avoid the opportunity for malicious activities. The extent to which this control is worth implementing does depend on the risk assessment and the size of the organization. At the very least, staff who are being disciplined, or who are on notice, should not be allowed into secure areas unsupervised. This also reduces the health and safety risk for a lone worker, who might have an accident or become ill in an area to which first-aiders may not have access without one of a restricted number of authorized staff being available to open secure doors.

- Vacant areas should be kept locked and periodically checked. This activity should form part of the schedule of activities of a security guarding company or individual guard.
- Personnel of contracted third-party service providers should be given only restricted access to secure rooms, and this should always be under supervision.
- Recording equipment (mobile phones, cameras, videos, photocopiers, etc) of any sort should not be allowed within secure areas; the records could (accidentally or deliberately) come into the hands of someone who wants to gain unauthorized access to the organization's sensitive information.
- Additional security restrictions may become necessary when the organization is working, in a specific area of its site, to develop something that needs to be kept confidential for a period of time.
- Finally, specific controls might be necessary to ensure that personal mobile devices (eg smartphones) or other recording devices (digital cameras, handheld video cameras, USB flash sticks, smart spectacles, etc) do not collect information from secure areas.

Delivery and loading areas

Control 11.1.6 of ISO27002 says the organization should control delivery and loading areas as well as any other areas to which unauthorized persons (such as members of the public) might have access and, if possible, to keep them isolated from information processing facilities in order to limit the danger of unauthorized access to those facilities. This control will have a different importance for different types of organization. A manufacturing or retailing organization is, for instance, likely to have more significant public access, loading and delivery issues than a straightforward office-based organization. The risks range from unauthorized personnel (customers, delivery drivers, etc) to dangerous deliveries (eg bombs, anthrax), any of which might compromise the organization's information security. A risk assessment should, as with every other area to be controlled, be used to determine the security requirements.

The measures that ISO27002 wants to be considered are as follows:

- Access to a holding area from outside the secure perimeter should be restricted to identified and authorized delivery staff or other personnel.
- The delivery and holding area should be designed so that delivery staff cannot gain access from it to other parts of the building.
- The external doors of a delivery or holding area should be closed when the internal one is open.
- Incoming material should be inspected for potential hazards or threats before it is moved elsewhere or to the point of use.
- Incoming material should, if appropriate, be registered on arrival.
- Incoming and outgoing shipments should, where possible, be physically segregated.

Implementation of these measures can require significant reorganization of existing delivery facilities and procedures with potentially a significant capital expenditure on the physical set-up. The risk assessment should reflect the fact that as security controls are improved in other parts of the organization, so remaining vulnerabilities become more significant because they provide the few remaining ways in which unauthorized access to information can be gained. In other words, once an organization has started down the road to ISO27001, it should be thorough and complete the journey.

16

Equipment security

Control A.11.2 deals with equipment security. It says the organization should take steps to prevent loss, damage, theft or compromise of its assets and the consequential interruption to its activities. It is broken down into nine sub-clauses, each of which deals with aspects of equipment security and disposal.

Equipment siting and protection

Control A.11.2.1 requires equipment to be sited, or protected, in such a way that risks from environmental threats and hazards, or unauthorized access, are reduced. ISO27002 identifies a number of measures to be considered, including the following:

- Equipment should be sited so as to minimize unnecessary, unauthorized access into work areas. For example, refreshment units or office machinery designed for use by visitors to premises should be sited within a designated and supervised public area; unauthorized personnel should not have to access secure offices in order to use these facilities. How visitors access toilets will need consideration. Clearly, if the only toilets are within a secure area, visitors will either have to be denied the use of them or will have to be escorted at all times! Doors to computer rooms should have, depending on the risk assessment, mechanisms for ensuring that they are kept shut and locked at all times, with any deviations notified on an alarm system.
- Information processing and storage facilities handling sensitive data should be positioned so as to reduce the risk of being seen by members of the public while in use. This applies, for instance, to workstation monitors in a ground-floor office, where passers-by could look through a window

and see what is on the screen. (Alternatively, windows could be screened.) This may not be relevant if the information that is likely to appear on the computer screen is not sensitive, but if it is, a simple solution might be the installation of window blinds. This would also apply to a wall or floor safe, in retail premises, which has been located so that it could be seen by a member of the public on the premises – it should be hidden in another room. Entrances to computer server rooms, and the security locks that protect them, should not be visible from the street, or through a window that would enable someone with a telescope potentially to see a code being input into a door lock. It all depends on the risk assessment; one should be carried out for each circumstance in which this control might need to be implemented and action then taken in the light of that assessment and in proportion to the risk identified. Decisions should, as usual, be documented.

- Items requiring special protection should be isolated so as to reduce the general level of protection required. Only a risk assessment will establish what type of equipment falls into this category; it is clearly sensible that, for instance, the fuse board that controls the power into the computer server room should be sited away from public places and away from places that even authorized staff access on a regular basis. An opportunist thief passing an office containing a notebook that is docked at a workstation but not otherwise secured might find it difficult to resist the temptation to add the notebook to his or her own briefcase.
- ISO27002 suggests that measures should also be adopted to minimize the risk of potential threats including fire, theft, explosives, smoke, water (or supply) failure, dust, vibration, chemical effects, electrical supply interference or failure, and electromagnetic radiation! The only way this can be complied with is to consider, in respect of each of the major systems and components of systems (see Chapter 6), what the risk of compromise will be for each of the risks identified in this section and, in the light of that assessment, to implement appropriate controls. Many of the controls that will be adopted will be simple common sense. Certainly, in any office environment consideration should be given to how workstations and, in particular, notebooks can be locked down so that they are not easily removed. Notebooks should, at the very least, be attached to the desk by notebook security cables, which have individual pass codes. There is a range of security products available, from a number of different suppliers (their advertisements can be found in most information security magazines), that are designed to secure equipment.

These range from night safes for notebooks through security ties for workstations to safes of one sort or another. There are sufficient security products available for any piece of important equipment to be adequately secured such that there is little real risk of its being stolen, other than by properly equipped criminals who are ready, able and determined to overcome the controls that are in place.

- ISO27002 recommends that an organization should consider its policy towards eating and drinking in proximity to information processing facilities. Most IT specialists will probably say that eating and drinking should not be allowed anywhere near IT equipment. Somehow, sometimes, this does not also apply to them! Direct experience suggests that very little of any real significance ever happens in the general office as a result of people eating or drinking at their desks. Sometimes, paper-based information is damaged, but computers rarely are. The debris left by people eating in the office can attract rodents and often leaves unattractive odours, but these tend to be the limits of their impacts. The one place where eating and drinking should certainly be banned (apart, obviously, from clean facilities or anywhere that is specifically designated as a clean area) is the server room. Eating and drinking inevitably leaves debris, which, because the server room is not (or should not be) accessible to the cleaners, accumulates and can have a negative impact on stored data or the machinery. Eating and drinking are obviously never allowed in clean rooms or similar facilities.
- Environmental conditions should be monitored for conditions that adversely affect the performance of information processing equipment. The organization should be particularly concerned here with heat and cold, smoke, dust and rain. IT equipment should not be exposed to any of these; server rooms should be equipped with detectors of heat, condensation or moisture, fire and smoke that have alarms that contact duty personnel (wherever they are – that is, the alarms must be able to trigger pagers or similar long-distance communications tools) who know what action to take to deal with the threat. Fire suppression equipment could also be installed.
- Lightning protection should be installed in all buildings that operate information systems and there should be lightning protection filters on incoming power and communications lines.
- Special protection methods, such as protective keyboard membranes, might be necessary for equipment in industrial environments.

- The impact of a disaster in nearby premises or sites (such as the street) should be considered.
- The danger of information leakage due to electromagnetic emanation should be considered. This includes the possible disclosure of information through unintentional radio or electrical signals, sounds or vibrations. 'Emission security' or EMSEC deals with this specific area.

Supporting utilities

Control A.11.2.2 of ISO27002 says the organization should protect its equipment from power failures, failures in supporting utilities and other electrical anomalies. This is obvious common sense, as all information processing equipment is electrically powered and is dependent on one or more of water supply, sewage, heating or ventilation and air-conditioning, but most organizations make inadequate contingency plans to deal with power failure. All support utilities should have a rota of regular inspection by an appropriately qualified engineer to ensure that they are still operating as required and are likely to continue doing so. For a start, every item of equipment should have a power supply that conforms to its maker's recommendations.

An uninterruptible power supply (UPS) is essential to support equipment running critical business applications.

The UPS should enable continuous running or, under specific circumstances, orderly shutdown. The UPS will need to be of adequate power to support the equipment that relies on it for as long as necessary to allow orderly shutdown or the provision (if possible and appropriate) of alternative power, and if necessary the manufacturers of both should be consulted. There should be contingency plans for a failure of the UPS. These might include provision of a back-up UPS. UPS equipment should be regularly tested in line with the manufacturer's recommendations and it should certainly be stress-tested in a simulation of the worst possible combination of power and service interruption circumstances that can be dreamed up, to ensure that the continuous running or system shutdown plans work effectively.

UPSs must also be considered for workers in home offices. Appropriate equipment needs to be provided to home office users to ensure that data are not lost. This might include USB sticks or other external memory devices, supported by a standard procedure requiring home office users to take at least daily back-ups of data. Users (both in the home office and mobile users,

with notebooks) should be trained to save the document on which they are working manually at predefined intervals or, alternatively, to have an autosave facility that does this; this will reduce the amount of work lost in the event of a sudden power outage, battery failure or finger error.

Home office UPSs also need to be tested on a regular basis, and a procedure for doing this will need to be designed and implemented.

A back-up generator should be considered if processing has to continue through a prolonged power failure. Just like the UPS, back-up generators should be regularly tested and stress-tested. Adequate petrol or diesel supplies should be immediately available and stored in accordance both with applicable health and safety legislation and with the outcome of a specific risk assessment.

While we deal later, and at length, with business continuity planning, this is an appropriate point at which to suggest that consideration might also be given to the impact a power outage could have on the working environment. In winter, a building will rapidly become too cold for staff to continue working unless alternative sources of heat are easily accessible and ready for use when needed; a visit to the local camping or plant hire shop should offer some ideas for solutions.

In addition, emergency power switches should be located near emergency exits in equipment rooms to facilitate rapid power-down in the event of an emergency. Emergency (non-electric) lighting should be available in the case of mains power failure at night or in winter. This may be no more than will be sufficient to enable the computer room to be secured and other secure areas or rooms also to be secured. Torches, issued to identified personnel and maintained in a state of constant readiness, may be sufficient; it will all depend on the risk assessment. Gas-operated lamps may also be required.

Lightning protection should be supplied for all buildings, and lightning protection filters should be fitted to all external communication lines. This can be particularly challenging for external communication lines that are without the control of the organization, and due consideration will have to be given to appropriate contingency plans for circumstances where there is a power interruption as a result of a lightning strike to a utility company's unprotected lines.

Finally, consideration needs to be given to all the other supporting services; critically, air-conditioning, humidification and fire suppression equipment needs to be regularly tested and have appropriate alarms fitted to alert staff when it has become inoperative. Telecommunications services

should have two different methods of connection to the service provider, to ensure that there is no single point of failure for a critical service, and there should usually be an analogue telephone service available as well to deal with emergencies where the digital service is unavailable.

Cabling security

Control 11.2.3 of ISO27002 looks to protect any cables that carry data or that support information services from interception or damage. With a bit of luck, some of the measures recommended by ISO27002 will have been implemented at the time your building was put up, because if they weren't, it is going to be difficult to implement them now. The measures ISO27002 wants to be considered are as follows:

- Power and telecommunications/broadband lines into information processing facilities should, wherever possible, be underground or subject to alternative adequate protection. If they are not already underground, it is probably too late. However, it may still be possible to ensure that cables are adequately protected. Specialist information from the utility company concerned will be necessary to help identify a way to protect them. Seriously, where highly sensitive data are being handled, the way in which the utility company handles its telecommunications cables may be critical. Where the risk assessment highlights this issue, there should be a discussion with the utility company about what extra protection it could provide. This protection is important; facilities that are otherwise protected could be penetrated simply because it is possible to tap into the telecommunications cable or cut the power cable. The sheer difficulty in implementing appropriate controls means that this becomes a particularly vulnerable area as everywhere else becomes more secure.
- Cabling in work areas should be appropriately organized and protected. The tangle of cable that often hangs out of the back of workstations and lies around on the floor is vulnerable to breakage and can, of course, be a health and safety risk. Cables should be tied away with cable tidies, power splitter boxes should be sensibly sited and, where possible, desks with cable handling systems should be used.
- Network cable should be protected by using conduit or avoiding routes through public areas. This is a lot simpler to bring about; the network cabling contractor can be instructed to install new cabling – or to strip

out and reinstall old cabling – in such a way that it will be protected from unauthorized interception or from damage.

- Power cables should be separated from communications cables to prevent interference. While the risk of electric interference is self-evident, keeping the two services clearly separate ensures that the risk of losing both power and telecommunications simultaneously is reduced.
- There are additional measures that should be implemented for particularly sensitive data: armoured conduits, locked rooms or boxes at cable inspection and termination points, fibre optic cabling, electromagnetic shielding, sweeps for unauthorized devices attached to cables, and controlled access to patch panels and cable rooms. Risk assessments should be carried out and expert advice taken, and measures that are identified as necessary through this process should be implemented.

Equipment maintenance

Control 11.2.4 of ISO27002 says the organization should maintain all its information processing equipment in accordance with the manufacturer's instructions and/or documented organizational procedures to ensure that it remains available and in working order. This clearly means that the organization should retain copies of all the manufacturer's instructions and should identify the recommended service intervals and specifications, and to enable a quick call-out for corrective action in the event of a breakdown they should be displayed together with the supplier's contact details on the equipment. Only authorized and trained personnel should carry out repairs or services; records of all work done should be retained (in an old-fashioned book attached to the machine) and there should be appropriate procedures (dealing with the saving, deleting or erasing of data, particularly sensitive or confidential data) for controlling equipment sent off-site for repair. Any insurance requirements should be identified and complied with.

There is a more important issue with older or legacy equipment. Equipment that works faultlessly for long periods can suddenly fail. It is important, at that point, that there are detailed records of qualified maintenance and repair organizations. More sensibly, a documented record of the service history of equipment should be maintained so that as it becomes older, properly informed decisions can be taken about the right time for it to be replaced.

Removal of assets

Control A.11.2.5 requires the organization to ensure that no assets – equipment, information or software – are removed from its premises without authorization. This is clearly a basic control that is useful in deterring theft of assets. The procedure for obtaining authorization (and the identity of those where are empowered to provide authorization) should be clearly laid out in the ISMS, and the steps that are required should be proportionate to the sensitivity or value of the asset. Valuable assets should be logged out of the premises and logged back in again; staff who are regularly carrying valuable assets in and out (such as notebook computers) should perhaps have written authority to do so, which they should carry with them at all times and be able to provide on challenge. Of course, the proliferation of mobile devices may mean that a number of individuals are issued with them as part of their basic employment contract and, therefore, some more sophisticated method of tagging might be required. It has to be recognized that, in detail, the guidance of ISO27002 is difficult to apply in an environment where mobile devices are ubiquitous; smart organizations will want to consider options for tagging mobile devices to identify cards. Spot checks should take place to detect unauthorized removals, and all staff and contractors should be made aware of this policy and that breach of it may be considered a disciplinary matter, perhaps involving the police. Remote workers who have company assets at home should be required annually to endorse an inventory of items in their possession, commenting on their current state of repair.

Security of equipment and assets off-premises

Not surprisingly, control A.11.2.6 requires the organization to apply security procedures and measures to secure equipment used outside an organization's premises. In particular, use off-site of any equipment should be formally approved (particularly notebooks, and smartphones, together with any other information processing equipment that will be used away from the office) by line managers. The process for this approval should be standardized and can be determined in the light of a risk assessment that considers the possible risks to the organization of its equipment when used off-site. Some of the measures that ISO27002 says should be considered are as follows:

- Notebook computers, USB sticks and smartphones should be encrypted, particularly if they contain sensitive information or personal data. Equipment (and media) taken off premises should never be left unattended. Notebooks should always be carried as hand luggage and, wherever possible, disguised. Notebook computers or USB sticks should not be left in cabs, on planes or anywhere else – but they often are, and the organization needs to think through the consequent risks. Possible controls include placing a limit on the data that can be carried on the C: drive of a notebook, requiring back-ups to a USB stick to be carried out at regular intervals, signing up for a web-based incremental back-up service, and limiting the period of time that confidential information can be stored on the notebook. Preferably, password protection (including screen savers) should be standard, and confidential information should be encrypted. Mobile devices should be backed up regularly, and access to both smartphones should be restricted by means of access codes.
- Staff should be trained in how to protect equipment from risks identified by the manufacturer, such as electromagnetic fields, and these requirements should be built into the user authorization requirements. While the idea of creating rules for handoffs between staff in relation to custody of mobile devices seems intellectually interesting, the reality is that devices will be lost or mislaid and, therefore, building remote wipe into the mobile device policy may be a more pragmatic solution to this issue than an exchanges log.
- A risk assessment in respect of home working should lead to designation of standard – and, where necessary, special – measures, such as lockable filing cabinets.
- Certainly, adequate insurance should be taken out to protect equipment off-site and this should be from an insurer that properly understands the market and offers cover adequate for the risks identified in the risk assessment.

Secure disposal or reuse of equipment

Control A.11.2.7 requires information and licensed software to be erased from equipment prior to its disposal or reuse. The standard 'Delete' function in software packages is inadequate; when equipment is to be disposed off, it

should be completely wiped of all data. Even so, the data image may still be on the disk. As disk drives are so inexpensive now, it may be better to destroy disk drives completely before selling PCs. Storage devices (USB sticks, tapes, CD-Roms, smartphones) should, for preference, be destroyed rather than reused. Workstations, servers and laptops should have their hard disks comprehensively overwritten prior to their disposal, and all software should be removed. Organizations that offer to destroy hard drives prior to disposing of PCs should be able to provide hard evidence that they do actually do this. Software may be copied and sold; the original licence holder for the software could thus be open to a charge of illegal software copying. Destroy any software before disposing of the hard media. Ensure that compliance with any Waste Electrical Equipment regulations also provides for secure disposal of information assets.

There also need to be specific procedures for ensuring that portable equipment is recovered from staff who leave. The best way to do this is to withhold final salary payment until all company property is returned. The only way to set this up properly is to have this specific right written into employment contracts initially. Indeed, subject to the value an organization puts on the data accessed by an employee during day-to-day activities, it may be sensible to alter a person's duties at the point of resignation. Removing the right, as well as the need, for a departing salesperson to access sensitive client data has obvious benefits. The early retrieval of company assets from such staff will also assist both the organization and the individual concerned – and will prevent any untoward suspicion if an asset is stolen, damaged or corrupted during the notice period.

Unattended user equipment

Control A.11.2.8 requires users to ensure that unattended equipment has appropriate protection. The primary focus of this control is workstations or servers that are logged on and then left unattended, usually temporarily, by the user. This offers an unauthorized user the opportunity to access resources or assets using someone else's user name, resources or assets that he or she may, in fact, not be authorized to access in the first place.

The need for server rooms to remain locked when unattended has already been discussed. All workstations, notebooks and servers should, however, have password-protected screen savers. These are set up by the user and should be set so that the screen saver fires up after a short period – three to

five minutes might be the maximum period. Otherwise, users should be trained to trigger the password-protected screen saver when leaving their workstation for any period of time, to log off when they have finished working on a particular application and to ensure that the log-off procedure has completed before any machine is switched off or left unattended. A regular audit of machines to ensure that they have been logged off, and not simply had the screen switched off, is a key part of maintaining this control.

Clear desk and clear screen policy

Control 11.2.9 of ISO27002 says the organization should implement a clear desk and clear screen policy to reduce the risks of unauthorized access to, or loss of, or damage to, information. This requirement should be contained in the user access authorization document.

A clear desk policy is one of the easiest to adopt. The first step is to ensure that appropriate facilities are available in the office in which, depending on their security classification (see Chapter 8), computer media (disks, tapes, CD-Roms) and paper and paper files can be stored and locked away, including in lockable pedestals, filing cabinets and cupboards. Sensitive information should be locked away in a fireproof safe (and the security adviser will have to assess the fire resistance of the safe in terms of the sensitivity of the information inside it and its location in order to ensure its survival for long enough to be rescued). Once the facilities are available, senior managers simply adopt a 'black bag policy'. The way this works is that after 24 hours' due notice that the clear desk policy will be implemented, senior managers simply go around the office after closing time and put everything that has been left out on desks into a series of black plastic bags. The bags are then left with the rubbish that the cleaners will remove for pulping the next morning. The first time this happens, the bags might be left briefly in the morning for people to recover the papers that they need. The second night, there is unlikely to be anything left out on desks to put into the black bags.

Personal computers, computer terminals and printers should be switched off when not in use and should be protected by locks, passwords and the like when they are in use. Everyone should be required to use a password-protected screen saver that automatically fires up after only a few minutes (between three and five is reasonable) of inactivity; this ensures that sensitive information is not easily available to the casual observer. While everyone

in the office should be trained to switch machines off, the last one out of the office each day should be required to double-check and switch off anything still on.

Incoming and outgoing mail collection points should be protected or supervised so that letters cannot be stolen or lost, and fax machines (where they're still deployed) should be protected when not in use. Photocopiers should be switched off and locked outside working hours; this makes it difficult for unauthorized copying of sensitive information to occur. All printers, fax machines and should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays or on the scanner bed for the wrong person to collect.

17

Operations security

Control category A.12 has a number of major sub-clauses. The first of them is control A.12.1, which deals with operational procedures and responsibilities. Its aim is to ensure the correct and secure use of information processing facilities.

Documented operating procedures

Control 12.1.1 of ISO27002 says the organization should document the operating procedures that were identified as necessary in the security policy and which are being discussed at length through the pages of this book. As discussed in Chapter 3 (management system integration), the document control principles of ISO9000 are applicable to ISO27001, and all the operating procedures that are part of the organization's ISMS should be treated in accordance with these requirements, including appropriate management approval.

Again as discussed elsewhere, the best way to make the entire ISMS available to staff is through SharePoint and the best way to make it available to third-party contractors is through an extranet, or secure access to part of SharePoint. The key benefits of such an approach are that documentation can easily be kept completely up to date and users can be sure that they are seeing the most recent version of ISMS requirements.

While the organization will adopt those procedures that it finds most useful in implementing its information security policy, ISO27002 recommends that there should be detailed procedures and operations (or work) instructions (and the level of detail should be appropriate to the size of the organization, with more detail required for larger and more complex ones),

which should be worked out between the information security adviser and the responsible operational staff, for:

- Processing and handling information – which covers, in particular, confidentiality requirements and information classification.
- Back-up, which is dealt with in more detail in control A.12.3.1.
- Work scheduling requirements, explaining where necessary inter-dependencies with other systems (so that no one has to find these out the hard way) and earliest job start and latest job completion times (for instance, for back-up procedures).
- Instructions for handling errors or other exceptional conditions, including restricting use of system utilities, although the organization should have due regard for the comments in Chapter 4 and elsewhere about the need to recruit and retain an information security specialist who has sufficient skill and experience to respond flexibly to new and unusual circumstances. These instructions might, therefore, set out reporting requirements and general guidance, with more specific instructions for junior operatives and inexperienced staff to follow.
- Contact details and for accessing appropriate support in the event of unexpected operational or technical difficulties, and what records should be kept.
- Instructions for handling special outputs, such as special stationery, or what to do with failed output for special jobs. Uncontrolled versions of these instructions should be posted near the machines to which they relate.
- Detailed system restart and recovery procedures to follow in the event of system failure. These procedures should be in the ISMS, and controlled copies should be visibly posted near the equipment to which they relate, to enable them to be easily used when required.

There should also be detailed procedures (based on manufacturers' instructions or user manuals) for all the basic housekeeping functions, including computer start-up and power-down, back-ups, equipment maintenance, mail handling, computer room usage, etc. These procedures should, wherever possible, be reflected in visible reminders as to requirements, posted in the vicinity of where they are relevant. Staff should be trained in their use. Consideration should be given to the possibility that unauthorized staff could see these procedures, and therefore their classification level would be relevant to how they are posted.

Remember that overly detailed or infrequently used procedures are as likely to lead to problems as no systems at all. Organizations that outsource their IT services – bearing in mind the distinction that outsourced processes would be within the scope of the ISMS although the organization delivering them would not – should specify the requirement for proper and appropriate system documentation, to ISO9000 and ISO27001 standards, in the outsourcing contract. It might be appropriate to require suppliers of outsourced IT services to be certified to ISO20000 and, arguably, ISO22301 as well as ISO27001.

Change management

Control 12.1.2 of ISO27002 says an organization should control changes to its business processes, information processing facilities, operational systems and application software. These changes usually cause major disruption to the business even when they go well. Inadequate control of these sorts of changes is a common cause of system failures or vulnerabilities. As some banks can testify, the transition from test to production can occasion major, costly and embarrassing system outages. It is also a common cause of unnecessary expenditure. Formal, documented change control procedures need to be in place, which could be adopted from or be the same as existing project management or change control procedures within the organization. What is important is that for all changes to information processing equipment, software or security procedures, there should be a formal method of control, preferably within an appropriate project governance structure.

Procedural or process change is easy to control, particularly if the ISMS was set up with the information security management forum as the body that steers implementation of the ISMS. It will have to approve all procedural changes, which should be issued under formal document control and supported, where appropriate, by additional staff training.

Changes to operational programs and applications can have an impact on one another, and the change control process should ensure that this risk is considered. The specialist input of the IT manager, or vendor-certificated experts, should if necessary be considered as part of the change management process. There needs to be a clearly formulated policy dealing with updates, patches and fixes to major operational and application software; there may not always be a valid business or information security reason for making the upgrade, and therefore the organization's policy needs to set out the criteria for upgrade decisions and their timings.

In general, the change control procedure for operating programs and applications could be on a standard single-page document that includes:

1. an identification of significant changes, and the business reasons (including, if necessary, a cost–benefit assessment) together with a change log;
2. the planning process for testing changes and gaining user acceptance of the changed system;
3. an assessment of their potential (security and other) impacts, including their impacts on other operational or application software and any hardware changes that might be required;
4. formal approval for the changes to be made, and verification that information security requirements have been met;
5. communication to all relevant people of the changes, perhaps by means of copying, or e-mailing, to them uncontrolled versions of the change control form;
6. procedures for aborting, for rollback, and for recovering from planned changes that go wrong;
7. emergency procedures for recovering from incidents or errors.

On a more substantial level, any significant change to the network would necessitate a review of the main information security risk assessment in advance of the change. Provision should be made in the change control procedure to ensure that this possibility is considered. Any dependent records would need to be amended.

Organizations that have already adopted ITIL or COBIT should integrate the detailed aspects of this control into their existing change management process; it makes sense to have a single, coherent, secure process for managing the whole range of changes that might need to occur.

Capacity management

Control 12.1.3 of ISO27002 says the organization should monitor its capacity demands and then to make projections of future capacity requirements so that it can ensure that it has adequate power, bandwidth and data storage facilities available. The utilization of key system resources (file servers, domain servers, e-mail servers, printers and other output devices) should be monitored so that additional capacity can be brought on-stream when it is

needed or capacity-hungry activities schedule for other times. The projections should obviously take account of predictions of levels of business activity, and there should therefore be an overt link between this activity and the annual business planning cycle. The trends that should be considered are the increase in business activity, and therefore in transaction processing; and the increase in the number of staff, and therefore in the number of workstations and other facilities. E-commerce businesses should also consider the expected increase in website activity and plan sufficient capacity to ensure that the site remains operational, particularly at times of peak activity.

All of this should enable network managers and webmasters to identify and, through their capacity management plans – including deleting obsolete files and data, decommissioning devices that are no longer required, scheduling bankwidth availability, etc – avoid potential bottlenecks that could threaten system security or the availability of network or system resources or data.

Separation of development, testing and operational environments

Control 12.1.4 of ISO27002 says the organization should separate development and testing environments (recognizing that visualization enables multiple environments to reside on a single box) from its operational (production) ones in order to reduce the risk of accidental change or unauthorized access to operational software and business data. This clause will be relevant primarily to software development companies and secondarily to any organization that is having bespoke software developed in-house for use, rather than buying a commercial off-the-shelf (COTS) package, in its own operations.

This is a key segregation of activities; the rules for the transfer of software from development to operational status should be defined and documented. ISO27002 sets out very clearly the ways in which software development should be separated from operations; any organization that is involved in developing software should refer explicitly to clause 12.1.4 of ISO27002 for guidance on best practice in how to do this.

Many companies that are not software companies are likely to be doing some limited development work even if it is limited only to process automation or website scripts. The controls of this clause of ISO27001 are also relevant in these circumstances. In essence, the requirement is that developing

and testing activities should be separated to the greatest extent possible, preferably running them on different computers or on different domains, and certainly running them in different directories. Access methods and passwords should be different between development, test and operational environments. The test environment should be a known, stable one, which emulates as closely as possible the live, operational (production) one and in which meaningful testing can take place and any attempt by a developer or webmaster to introduce malicious code or Trojans or build-in vulnerabilities can be detected. Users should have different user profiles for testing and production environments, and developers should never have access to the live site or production environment.

There are also specific data management issues to be considered in regard to the use of personal data for testing; all personal data, even those used for testing purposes, are subject to the DPA 2018 or other privacy regulations.

Back-up

Control A.12.5 requires the organization to take regular copies of essential business information and software. This is one of the most basic and most important of all controls. It is important not just because it enables an organization to recover from a disaster or media failure, but because it can also enable individual users to recover from unforced errors. Where back-ups have not been taken, it can be impossible to recover from disaster. This is as true for a cloud-based business as it is for one that runs its own server room or data centres; cloud back-ups that are stored behind the same dashboard as the core configuration and other data are just as exposed – and as potentially useless – as back-up media stored alongside their servers in a physical location.

An essential first step in making a back-up policy work in most offices is to ensure that most information is filed on the organization's servers, or network drives (whether onsite or off) and not on individuals' C: drives. While servers can be backed up automatically and centrally; C: drives can only be backed up if the back-up service is specifically configured to do so. This is difficult to do with tape back-up services, and is particularly difficult with notebook users, who often work on the move and who need immediate access to their files. The requirement for regular back-ups from portable devices to network file servers or the Cloud (or the provision of notebook-level back-up service) and for the use of the Cloud or a file server rather than

the fixed C: drive should be part of the initial staff training on data security. One step that might be considered in order to illustrate the importance of this particular control might be to make unbacked-up storage of digital data on a desktop a disciplinary offence.

A second essential step is ensuring that the back-up policy is comprehensive. Mobile users have information stored in notebooks and on smartphones. Office-based users use a range of software products, sometimes on single machines only, which might be outside the normal range of Microsoft products. Organizations have websites, intranets and extranets. They use accounting systems, ERP systems and project management systems. They have voicemail systems, which also carry data, particularly in all those voicemail boxes that substitute more and more for real people. Increasingly, organizations use the services of application service providers (ASPs) and SaaS (with the use of applications like Saleforce.com (archived at https://perma.cc/4QKH-A6YZ) and Office365 becoming widespread), and this leads to data being stored outside the organization's secure perimeter in situations where the organization has no direct control over the security of its information. It is critical, in these relationships, that the controls for security in third-party relationships discussed are carefully considered. All digital data storage needs to be considered – and so do paper files.

The fact that data are stored in paper files or in other books does not make them any less important to the organization than data in digital form. A fire, a flood, an explosion or even simple straightforward theft can deprive an organization of its paper files. They need to be taken into account, and those that are assessed as important to the organization need to be backed up in some manner; the great fire of Alexandria destroyed many original manuscripts of which there were no copies anywhere else in the world.

Once the organization has identified all the data assets that need to be backed up, it can decide on a method, and frequency, for carrying out the back-up. This exercise should be comprehensive and should link back to the list of assets that was put together as part of the initial asset inventory. Each of these methods of backing up and storing data should be risk-assessed in the light of the highest security classification that is likely to be given to data stored in this medium or a particular file or device. There is an early decision to make, for electronic data, between dual-writing (making the copy at the same time as the original) and once-per-day copying. Once a decision has been made as to what data are to be protected, and the necessary level of back-up information has been defined, the controls that ISO27002 would like to see considered are as follows:

- The minimum level of back-up information, together with accurate and complete records of what has been backed up and a copy of the documented recovery procedure, should be stored at a remote location. Accurate records of what has been backed up are necessary to facilitate finding what is required for a restore operation. The minimum information would be details of precisely which servers have been backed up and the date and time of back-up. It does need to be sufficiently remote that if, for instance, the base city ceased to exist, the remote site could take up the burden. The remote location should be sufficiently remote to avoid any disaster that takes place at the main site (or that affects the environs of the main site) but not so remote that it cannot be easily accessed. Back-up tapes might also be stored with a storage company, which collects one tape (or set of tapes) every day and leaves behind the next tape (or tapes) in the cycle. The contract with such an organization would, of course, be subject to the organization's standard controls for third-party contracts. At least three cycles of back-up information should be retained for important applications. A typical back-up cycle, of digital media to a digital audiotape (DAT), is called 'grandfather, father, son'. These three generations refer to monthly, weekly and daily back-ups, with the 'son, an incremental back-up running every day (one tape for each day of the week) and being overwritten on the same day the following week. The 'father' back-ups are full back-ups done every week (one tape for each week of the month) and then overwritten in the same week of the next month. The 'grandfather' back-ups are done every month (one tape for each month of the year) and overwritten in the same month of the next year. Autochangers and additional software might be necessary to ensure that back-ups are done fully and effectively.
- Back-up information should be given the same level of physical and environmental security as the original data; it is just as important, and therefore standard physical and environmental controls must also apply to the back-up data. Where necessary, back-ups should be protected by encryption.
- Back-up media (eg the tape unit) should be regularly tested to ensure that they are working. The back-up should be set to happen at a regular time each 24 hours, or whatever shorter or longer cycle the organization chooses in the light of its assessment of its risks of data loss. It should take place at a time of limited or zero network usage, as the network will run slowly while the back-up takes place and those sections being backed

up are unlikely to be available to users while the back-up is taking place. It should be demonstrated that the equipment and media used have the actual capacity to complete the required back-up within the allotted time. If they do not, the back-up may be flawed and critical data may be lost. Details of these tests should be retained with the ISMS documents and are critical evidence that the back-up system will be able to help when it needs to.

- Recovery and restoration procedures, which should be documented in the ISMS, should be regularly tested. The testing should involve those staff who will be responsible for carrying out the restoration, as it is critical that restoration can actually be completed within the time allotted. Tests should be carried out to restore data from every single one of the servers and for every single one of the applications that are supported, and restoration should be to vanilla boxes; it is only through such exhaustive testing that the organization can be sure that it will have what it needs when it needs it. Deficiencies should be put right either through training or through reassessing the software, hardware or back-up procedure itself. The wrong time to discover the deficiencies in this procedure is in the middle of an attempt to restore either an important document or an entire system. The records of these tests, and their outcomes, should form part of the ISMS business continuity documentation. Like all critical tests, they should be reviewed by the information security management forum on a regular basis. Restoration of files from historic records will become increasingly difficult as organizations update or change their software; they will need to remember to retain the ability to access old electronic records for as long as their data retention policy requires, and that this might necessitate retention in a working state in a secure environment of software that has otherwise been superseded.
- Critical paper files should also be backed up, with complete photocopies stored at a remote location. The comments about physical security for back-up documents, and controls over copying paper documents should also be applied.
- RAID (Redundant Array of Independent Disks) should be considered for all servers running critical applications. This will provide a level of protection if one of the server drives fails. There are seven (0–6) basic RAID levels, providing different levels of data protection and performance improvement. A risk assessment should be the basis on which selection and implementation of a RAID solution takes place. RAID 5 is the usual

level of RAID array implemented, and this combines a good level of protection and performance. Expert advice should be taken on the implementation of a RAID array.

- The retention period for business information should be defined and applied to the backed-up data. It is particularly important to recognize that legal requirements now increasingly require that e-mails are retained as business records. Data vaults and single-instance e-mail storage may be appropriate solutions to this requirement.

Mobile device back up is increasingly critical to organizations and decisions made about how this is to be effected should be part of the mobile device policy and procedures. As the fundamental controls that protects an organization against compromise of critical or sensitive data on laptops or mobile devices should now include some mix of boot-level whole disk encryption for laptops and remote wipe for smartphones and similar mobile devices, it is essential that organizations implement some form of ongoing, incremental background data and system synchronization to some easily accessible – but significantly secure – central repository.

Chapter 24 deals with A.12.4, logging and monitoring, alongside information security incident management.

18

Controls against malicious software (malware)

Control objective A.12.3 requires the organization to protect the integrity of software and information by implementing detection and prevention controls against malicious software and to ensure that appropriate user awareness procedures have been implemented. The importance of this control was highlighted by a finding, as long ago as the FBI/CSI 2002 survey, that 85 per cent of organizations had detected computer virus threats. Year after year, similar surveys produce similar results: the 2014 ISBS survey found that 73 per cent of large organizations (up from 59 per cent the previous year) had suffered a malware attack. More recent surveys all indicate similar levels of suffering. Many organizations think that because they have some form of anti-malware software in place, they have a data security system. They don't. This book, and ISO27001 itself, makes it clear that anti-malware controls are just one part of an effective data security system; they are, however, an extremely important part.

Viruses, worms, Trojans and rootkits

An overall understanding of the world of computer malware, the different types of virus and their characteristics, would be useful ahead of a discussion of how to resist them. Technically, the most useful generic term to use is 'malware', a term that denotes software designed for some malicious purpose. It may be written in almost any programming language and carried within almost any type of file. Common forms of malware include viruses, worms, Trojans, spyware, adware, bugs and rootkits. 'Antivirus' and 'anti-malware' are terms that are used interchangeably in this book.

A virus has at least two properties: it is a program capable of replicating – that is, producing functional copies of itself – and it depends on a host file (a document or executable file) to carry each copy. It may or may not have a 'payload': the ability to do something funny or destructive or clever when it arrives.

A worm, however, is autonomous. It does not rely upon a host file to carry it. It can replicate itself, which it does by means of a transmission medium such as e-mail, instant messaging, Internet Relay Chat, network connections, infected websites, etc. Polymorphic worms are designed to evolve in the wild, to more effectively overcome evolving virus defences.

A Trojan is hostile code concealed within and purporting to be bona fide code. It is designed to reach a target stealthily and be executed inadvertently. It may have been installed at the time the software was developed; it is often the payload of an e-mail attachment or is designed to infect the computer of someone who clicks on a link in a phishing e-mail. The objective is often to achieve control over the target system.

Rootkits are pieces of software installed at the root of a system, either manually or automatically, hiding themselves carefully, enabling an attacker to have significant influence over everything that happens on the compromised system.

These definitions can overlap. Some malware can exhibit properties of both viruses and worms. Some worms deliver Trojans. Whatever the malware, it is usually a well-defined entity, within a single file or part of a file. However, new-generation malware increasingly involves cooperation between several entities split over several files.

Virus writers used to do it for fun, because they enjoyed the challenge of writing clever code, out of loneliness and a desire to have some impact on the world. Not so much anymore. Increasingly, malware is created by cybercriminals as part of an organized criminal activity. Criminals collaborate and have online groups, websites and communities through which they share work and ideas. They also compete with one another, and certainly their relationship with antivirus companies is often extremely hostile. Virus toolkits are now available online, so that anyone with limited code-writing skills can also create a virus; malware as a service is another option.

Increasingly, virus writers are cooperating with hackers and spammers. Spammers want to get their messages past corporate anti-spam filters; virus writers and hackers are good at breaking defences; and the spam industry is a very lucrative – albeit largely illegal – one. Of course, many electronic messages are actually simply virus delivery vehicles and therefore very

similar to spam anyway. And the environment is becoming ever more complex as 'mal-mailers' develop new ways of beating network gateway defences, and phishing and pharming e-mails are becoming seriously sophisticated.

The result is that in today's computer environment the only way to completely avoid the danger of malware getting on to the organization's network is to refuse to allow electronic access to the network. An internet connection, a USB flash stick or thumb drive, a CD-Rom reader, a floppy disk, an individual user – these are all possible sources of virus infection.

Most infection is accidental; in other words, the virus was not directed specifically at the now-infected organization. It just happened – someone clicked on a link on an infected site or opened an attachment in a phishing e-mail. Refusing access for everyone to everything is obviously not the business-oriented solution that might be expected from most risk assessments, and the extent to which gateway defences block legitimate e-mail ingress because it is carrying an Adobe attachment or download link suggests that most risk assessments are failing to consider the 'availability' aspect of information security: this is the digital age, after all, and most data is shared digitally, from White papers and e-books to software upgrades.

Spyware

Spyware (and adware) continue to be two of the most significant malware issues that organizations have to deal with. Spyware is software downloaded on to a workstation hidden inside a bundle of free software or adware. It is pernicious, and for users it creates significant issues in data protection and system availability. It can include Trojans and auto-diallers. Every organization needs a policy and procedures for dealing with spyware – not least because many antivirus vendors do not adequately deal with this threat.

Anti-malware software

The common solution is to install appropriate anti-malware software. Choosing anti-malware software needs to be done carefully, because poor software will not provide adequate coverage. Malware protection is a complex issue and is not easy for amateur users to navigate. It has been argued that it is probably impossible for ordinary users to perform a

meaningful anti-malware product test, to evaluate their comparative efficiencies or to carry out a quality evaluation of the many competing malware detection products. There is also not much correlation between price and quality where anti-malware software is concerned.

Anti-malware products need to be tested over long periods of time to ensure that they can handle the rapidly changing nature of the malware threat on an ongoing basis. However, most organizations need to make decisions about what to buy and install in much shorter time-frames. The vendor's own marketing material is, not surprisingly, an inadequate basis for choosing software. While there are some commercial approval schemes for anti-malware products, these usually only test detection rates without carrying out a proper scientific evaluation. They are therefore not the best sites to start with when choosing anti-malware software. One needs to obtain comparative test data for anti-malware products, and sites that produce this information should be the starting point for anyone who is making an initial or repeat assessment of these products and who wants to see data from independent lab tests.

There are probably only some three or four products that consistently perform well in these tests. An anti-malware product should be chosen from among these companies, all of which have the resources to compete and survive in this marketplace. Size of organization is not, however, a guarantor of anti-malware quality, and there are some substantial organizations that have detection rates consistently demonstrated as being very poor. Under no circumstances should a software product from a small or new producer be chosen either. The organization needs to have the resources to develop its technology. To research malware, to stay on top of developments in a dynamic environment, and to develop and produce countermeasures.

A website worth visiting is www.virusbulletin.com (archived at https://perma.cc/7NYS-JQXF), which publishes the *Virus Bulletin*. It contains single reviews of many anti-malware products, and occasionally comparative reviews. It contains up-to-date information about viruses, about spam, about new viruses and about methods of countering them. It contains a list of viruses live in the wild and has tables showing the prevalence of virus reports each month. It also has a list of hoax viruses; there are many hoaxes, and the sensible information security adviser will want to deal effectively with them.

Anti-malware software needs to be integrated with the network or system firewall and needs to deal with spam and instant messaging as well as being

capable of dealing effectively with endpoint security issues. The 'endpoint' is the point at which the organization's security potentially breaks down: the home worker's own computer, the laptop, the smartphone, the USB stick or even the digital camera or MP3 player.

Hoax messages and Ransomware

Virus hoax messages are becoming less familiar for all e-mail users, but one still needs to be aware of them. They play on people's ignorance. Users are understandably concerned about viruses, and so consider it 'helpful' if, as suggested by the majority of hoaxes, they forward the message on to their entire address book.

Such an action, although well-meaning, is not helpful. Aside from the imposed network load, the consequence is that the hoax becomes 'well known' and listed on web pages that list hoax viruses. This fame (of sorts) no doubt leads to some degree of satisfaction for the hoax perpetrator.

The organization should train all its users to respond appropriately if they receive a 'new virus' warning message. Warning messages encouraging the recipient to forward the information to all his or her e-mail contacts will typically be hoaxes.

Ransomware is, however, a whole different matter. It is a form of malware which restricts access to any computer system it infects, and demands a ransom – typically in the form of a Bitcoin or a creditcard payment – in order for the restriction to be removed. Cryptolocker and Emotet are examples of such products. Like other forms of malware, ransomware continues evolving and finds its way onto systems following much the same vectors as other malware.

Users should be required to report anything that looks like ransomware (and this includes malware that attempts to automatically install additional security software) to their help desk or security adviser immediately, by telephone or in person, and on no account should anything infected be forwarded, or copied on, to anyone, whether they are inside or outside the network.

Vishing (voice phishing) can be deployed by an attacker to dupe a target into installing ransomware or handing control of a computer to the attacker, using remote desktop access software.

Phishing and pharming

The last decade has seen an explosion in phishing attacks. Phishing, originally, simply involved attempts by cybercriminals to trick owners of bank accounts to input their secret personal authentication information into a site that looked like an official site. Early phishing attacks were crude, and poor spelling, inadequate grammar and odd syntax within the e-mail, combined with poor quality replication of an official website, easily identified these e-mails as likely to be fraudulent. These e-mails have, however, become increasingly sophisticated and look increasingly like the 'real thing'. What continues to give them away, though, is their existence – all banks are very clear that they will never send out e-mails asking people to input any personal information. Hovering over embedded links and sender e-mail addresses can also reveal the often minute deviations that indicate the e-mail is a spoof. Spear phishing are e-mail phishing attacks that look as if they really are addressed to you; 'whaling' is phishing aimed at senior executives and people in critical senior roles. They usually draw on information stolen elsewhere – such as birth date, or membership details from a hacked membership network, or personal data unnecessarily exposed on a Facebook page – to present themselves as more credible. Those that come from within the e-mail system of a trusted third party are very difficult to spot and, increasingly, effective and repeated staff training is the only way to deal with the phishing risk.

Pharming is the name given to the diversion of a website's traffic to a fake, malicious version of that website which tricks browsers into providing personal and payment card data thinking that they are still on the original site. The purpose of the malicious website is sometimes to install malware on the browser's computer, rather than to obtain information immediately. The existence of a valid SSL certificate on the website was usually the standard sign that the site is secure and staff should be trained to avoid using websites that don't have a valid, current SSL certificate. However, there is a possible SSL 3.0 vulnerability which attackers can, under certain conditions, exploit. Organizations that run SSL/TLS should take up-to-date technical advice to ensure they minimize their vulnerability to an exploit known as Poodle. Anti-malware software also provides no protection against pharming.

Anti-malware controls

ISO27002 recommends, in clause 12.2.1, a number of common-sense measures to limit the risk of malware infection:

- The ISMS should contain a formal policy and a procedure that requires compliance with software licences and that forbids the use of unauthorized software.
- There should be a policy that protects the organization against the risks of importing malware on disks, files, thumb drives or software that come from outside the organizational network. Such a policy has to be drafted in the light of a risk assessment and current technical advice about anti-malware capabilities, and is likely to be a combination of required activity and technical controls. This policy should, for any network deploying Microsoft products, take into account the security components of the Microsoft operating system, as it is important that the default firewall, antimalware and software automatic updates are configured correctly and in line with corporate policy. The policy could include disabling the disk and CD-Rom drives and USB ports on network PCs and notebook computers, requiring any data that arrive on such media to be loaded by an IT team that is able first to check the media for viruses. Alternatively, anti-malware software that is capable of checking files that are being uploaded from such sources could be deployed. The policy could ban downloads of software (such as screen savers and utilities) from the internet and/or set up controls on its firewall that make it impossible for such software to be imported, which automatically ensures that such downloads are not carrying malware. It could extend to making the unauthorized use (where the organization requires it, there should be a method for authorizing and verifying it) of external software a disciplinary matter.
- Anti-malware software should be installed on the network, and updates should take place in line with the vendor's update policy – which should be closely tied to the (we would hope, several times daily) availability of the updates. The ISMS should retain records of the planned updates and of their actual occurrence. The discussion, earlier in this chapter, about how to select anti-malware software is relevant here, as the evolution of malware happens quickly and leads the evolution of anti-malware products. Failure to update can expose the organization to severe threats, as new malware may be substantially more lethal than older variants.

It is important that appropriate consideration is also given to endpoint security: protecting notebook computers and mobile devices (particularly where they can be synchronized with data on the network such as diaries, contacts, etc). Wireless networks pose particular challenges, as there are airborne viruses that can infect them. In other words, anything that transfers a file, or a part of a file, is also capable of transferring malware, and appropriate technical support plus a risk assessment and the subsequent implementation of appropriate controls are necessary steps to ensuring that they are secured.

- All patches, fixes and service packs that are published by Microsoft on its website, and those published by other vendors for their products, should be applied as they become available. They are usually published to deal with either a bug or a known vulnerability that could be exploited either by a hacker or by malware, and if the malware does not already exist at the point the patch becomes available or the vulnerability is publicized, it soon will – sometimes within a matter of hours. There should be a record of what has been downloaded and applied, by whom and when.
- There should be a regular review of the software and data on all systems that support critical business processes. There is software that is designed to identify all software running on the system and this should be used to support the review process. The presence of any unauthorized files or software should be formally investigated, and if appropriate authorization is not forthcoming, they should be deleted.
- All files from external sources, particularly from non-trusted, uncertain or unauthorized sources or over non-trusted networks, should be checked for malware before use, and the organization should have a centralized, automated process for carrying out and documenting this check. The process needs to be intelligent if it is to be business focused; simply blocking all unknown senders is not helpful.
- All e-mail attachments, download links and software downloads (where permitted) should be checked for malware at the point of entry to the network: the firewall. Further checks against malware could and should be carried out on the desktop and on the servers as well. In other words, the anti-malware software should be installed on the print and file servers, the e-mail server and the workstations (integrating effectively with the endpoints), and all these should be kept up to date. A software package that enables updating to be driven centrally across the network is the most useful method of dealing with this.

- Users should be trained to recognize, and respond appropriately to, possible malware-infected e-mails. E-mails from unknown people, or e-mails from known individuals that either are unexpected or have unusual content lines, should be suspect. Virus writers play to the curiosity, fearfulness or egotism of potential recipients, and subject matter lines like 'Hi' or 'I love you' or 'This is approved' or 'Happy Christmas' are likely to mask potentially destructive viruses. The same e-mail message appearing multiple times from the same sender or from different senders is extremely likely to be a virus and should be recognized as such. User training should include *not* opening the e-mail at all, and using the organization's alternative, non-e-mail, incident-reporting procedure to report its arrival as fast as possible.
- There should be clearly documented management procedures that set out responsibilities for running the anti-malware software, for dealing with a malware incident and for recovering from one. Training in all these aspects should be carried out, and records of the training, which should be kept up to date, should form part of the ISMS records. A virus incident is a security incident and is covered as part of control 16: Information security incident management.
- There should be appropriate business continuity plans that enable the organization to recover from malware attacks. Back-up procedures are discussed in detail in a previous chapter.
- Information security managers should have appropriate sources of accurate and up-to-date information on malware, which they should use both to analyse incidents and to plan ahead to ensure that the organization avoids such incidents. The website www.virusbulletin.com (archived at https://perma.cc/7NYS-JQXF) was mentioned earlier. The organization might also subscribe to the twice-weekly *Security Wire Digest*, available by e-mail from searchsecurity.techtarget.com (archived at https://perma.cc/KZ3L-UZHK). There are other journals, magazines and sites that provide regular, up-to-date information, and the information security professional should ensure that he or she remains fully up to date.
- It is particularly important to have reliable sources of information about zero day attacks: those attacks which exploit a vulnerability before the software vendor is aware of it, or a patch for it has been figured out or distributed. These attacks can be aimed at widely used operating systems or at open-source software and can create significant challenges. Recent examples include Heartbleed. As the dark market offers substantial

bounties to researchers who are able to identify such vulnerabilities, this is security risk area to monitor continuously.

- Specific controls against spyware, incorporating both restrictions on what may be downloaded from the internet, and anti-spyware software, will be essential.
- Specific technical controls and training for dealing with malware-infected websites may also be necessary.

Airborne viruses

Smartphones and 3G/4G or web-enabled cellular phones (together often referred to as 'handhelds') are increasingly targets for hackers and virus writers. While there is still only a relatively small quantity of malware (Trojans and viruses) targeting handhelds in the wild, it goes on increasing. Mobile apps, however, particularly free apps written for the Android operating system, can be a practical attack vector, whether to collect in-app data or to transition to the network. Viruses can get from PDAs and into host computers, when PDA and PC files are synchronized. They can also transfer from PDA to PDA via infrared ports and Bluetooth technology. They can be picked up over the air, using wireless modems. They can spread by telephone connection, and smartphones are particular targets. However, the risk of damage to data stored on handhelds is still less than the risk of damage to networks as a result of viruses (written to be innocuous to handhelds but infectious to desktops and networks) that are transmitted to networks by handhelds when users synchronize PDAs and PCs. Handhelds that have wireless connections to the internet can be used to mount denial-of-service attacks, and could be used for defrauding phone networks or other malicious activity.

A bigger issue for smartphone users is the ease with they can be hacked, and the extent to which personal data – text messages, website transactions, location, etc – can be gathered by an attacker who has named a wireless network with something sufficiently similar for all nearby mobile devices that are set to 'automatically join networks' to join the attacker's. While this should properly be dealt with as part of the access control processes, it is important to recognize the seriousness of this threat for what it is.

Most users of handhelds are relatively unsophisticated in their understanding of malware and security issues and take little or no action to protect

their handhelds. Multiple platforms mean that it is difficult to produce generic anti-malware software. Handhelds are small, with relatively limited memory and processing power, which limits the options for anti-malware development. Free apps often come with their own brand of vulnerability. The only secure approach for the organization to adopt is a layered one, which installs anti-malware software on the handheld (the endpoint) to concentrate on the hand-held viruses, and to install an anti-malware solution on the desktop that scans handhelds during each synchronization. These needs will have to be taken into account when selecting an anti-malware package, and the network will need to be appropriately configured. Organizations should also consider, as part of the user access statement, including a warning about airborne viruses and the need for users to be alert to possible infections on mobile devices.

Control of operational software

Control 12.5.1 of ISO27002 says the organization should apply controls to the implementation of software in operational systems. This is an obvious need: organizations are vulnerable where unauthorized software is installed or updated, and the result could be loss of data or loss of integrity. Major new software packages should be rolled out only after they have been extensively tested against predetermined criteria, deployed by trained system administrators and authorized by management; underlying this should be a risk assessment. It is usually sensible to have planned fall-backs in place, including extensive copies of data, for roll-outs that affect the most critical of the organization's functions. Beware 'big bang' roll-outs where a whole new system is rolled out and goes live without having been extensively tested and stress-tested.

This book is written primarily for systems based on the Microsoft software suite, and therefore the best practice contained within ISO27002 regarding the deployment of software developed in-house will not be discussed here, other than to observe that it would be worth referring to ISO27002 if non-COTS operational programs are to be developed or deployed.

Vendor-supplied COTS software, such as that found on many organizational systems, should be maintained at the level supported by its supplier. This means that the organization should track upgrades and, as soon as it is satisfied that the upgrade is secure, should implement it. Patches and hotfixes should be applied as they become available, unless there is a significant

reason not to apply them. This can be established by reference to a vendor's website and to any of the regular information sources identified in Chapter 4. Suppliers should only be given physical or logical access to the software installed on the organization's systems with prior approval from the line manager and possibly the information security manager as well. The supplier's activities should be monitored. The organization must also decide who is to be responsible for ensuring that systems are updated, and this responsibility should be documented in line with the principles laid down in Chapter 4.

The organization should also ensure that all new software products (including upgrades) are obtained against an authorized and clearly identified business need and that adequate copies of the software licences are obtained for the actual number of users (ensuring that the right distinction is made between 'concurrent user' and 'per seat' licensing regimes).

The above control works together with that in A.12.6.2, Restrictions on software installation, which requires rules to govern what software users should be authorized to install on their workstations or devices. While the former deals with rolling out new software into the business environment, the latter deals with the installation of point solutions. ISO27002 suggests that users should only be allowed (and this means the limitation is embedded in their user profile) to download and install software that has a known and approved provenance, but be banned from installing anything suspect or which might come with malware.

The challenge, for most organizations, comes in extending this control to mobile devices which may now be the most vulnerable end points for the network.

Technical vulnerability management

Control 12.6.1 of ISO27002 is designed to ensure that organizations take adequate steps to prevent damage that could arise from the exploitation of published software vulnerabilities. There are regularly updated central stores of vulnerabilities at Bugtraq (www.securityfocus.com/archive/1 (archived at https://perma.cc/ZB2D-34QF)) and CVE (https://cve.mitre.org (archived at https://perma.cc/ZS35-2RNV)).

As was discussed in previous chapters, we live and work in an era when the elapsed time between publication (by the software vendor or, more likely, a third party) of details about a newly identified vulnerability and the

appearance of the first virus or hack to exploit it has reduced to a matter of hours, or less – what are called 'zero day' exploits. In this environment, organizations cannot afford to go without a policy and process for the timely, systematic, comprehensive and reliable updating of their systems with all patches and hotfixes issued by their software manufacturers.

Of course, the prerequisites for such a process are the asset inventory and a timely and reliable information alert system. The asset inventory needs to be complete and current, and needs to include adequate software information: vendor name and contact details; software serial number and version number; details of upgrades, fixes and hotpatches currently installed; and the person responsible for the item.

A four-stage vulnerability management system should be developed. It should ensure that vulnerabilities are identified, that a decision is made as to how to react to those vulnerabilities, that there is careful testing prior to patching and that actions are tracked so that success (or otherwise) can be monitored. This system should:

- Prioritize high-risk (see Chapter 6) systems.
- Prioritize high-risk vulnerabilities.
- Define roles and responsibilities with respect to vulnerability management, including monitoring and identifying (for all of the software and hardware) the vulnerabilities and release of patches, risk assessment, identifying the urgency with which the patch needs to be deployed, carrying out the actual update (refer to control A.14.2.2) and dealing with any coordination. There should be absolute clarity about accountability, and individual responsibilities should be clearly written into job descriptions.
- Identify, for each of the software and other technology items, the relevant source of information about vulnerability identification (possibly through Bugtraq or CVE) and patch release (usually the vendor website, or through use of an appropriately configured automatic update facility), and this information should be regularly reviewed and, where necessary, updated.
- Ensure that there are set steps, within a predetermined time line (such time line to be developed in the light of a process-level risk assessment), for identifying the risks of proceeding and of not proceeding with any given patch, for deciding what steps should be taken and for implementing that decision – which should usually be to install the patch unless there are good reasons not to.

- Allow, under certain emergency circumstances, the patch to be installed following the incident response process rather than the change management one; any such decision should be properly tracked and all the records updated appropriately.
- Ensure that, where necessary (the risk assessment process drives this), and prior to implementation, patches are tested and evaluated to ensure that there are no side effects on other systems.
- Allow, in circumstances where a patch for an identified vulnerability is not yet available or the side effects of implementing it are not acceptable, the organization to adopt alternative controls, such as turning off services that are affected by it, modifying firewalls or other access controls, increasing user awareness to detect and respond to attacks or increasing monitoring of activity to identify an attack on the vulnerability.
- Ensure that there is always an audit log of activity in relation to vulnerability management.
- Provide for regular monitoring and review of the vulnerability management process, not just through the internal audit function to ensure that it is working according to specification but also by the information security adviser to ensure that the specification remains adequate in the light of the organization's evolving risk assessment and risk treatment plan, in the changing security environment.

Information Systems Audits

Control A.12.7 is dealt with in Chapter 26, alongside technical compliance checking.

19

Communications management

Any organization that is pursuing ISO27001 is likely to be a reasonably complex one, with one or more networks of computers, usually across a number of geographic locations. Effective communication management – and therefore effective network management – will be essential to the stability of its operations, and therefore this is a key area for control. The ISO27000 family of standards includes ISO/IEC 27033 (a five-part standard) which can provide additional technical guidance on networking security.

Network security management

Control 13.1.1 of ISO27002 says the organization should implement a range of controls to achieve and maintain the security of information in its networks, particularly in those that span organizational boundaries. This is also designed to protect the supporting infrastructure and to protect connected services from unauthorized access. There are a number of components to making this control effective:

1. Following the principle of segregation of duties operational responsibility for networks should, wherever possible, be separated from computer operations. The organization should describe within its ISMS (perhaps through a minute of the forum, or the job descriptions of the individuals) how this is achieved.
2. There should be clear responsibilities and procedures for the management of networking and remote equipment, combined with logging and monitoring to identify any activities which may indicate a threat in action (suspicious data volumes, activity in unexpected sectors at unusual times, etc).

3 There should, if necessary (ie if a risk assessment identifies it as so), be special controls to protect data passing over wireless and public networks. These could include cryptographic techniques (eg encryption of data), controls to protect the network from unauthorized access (eg VPNs) and controls to maintain the availability of computers connected to the network.

4 Close coordination of management activity (a key role of the forum discussed in Chapter 4) should ensure consistent application, across the entire network, of the ISMS controls.

Neither the standard nor ISO27002 helps much in this section in terms of network management. This is partly because of the speed with which networking has evolved since the standard was drafted. Many of the requirements of this clause are met by controls introduced in response to other requirements of the standard, as indicated above. Network management is, however, one of the most critical roles within the organization, and, of course, how it is to be carried out does depend very much on the type of network that is installed. The architecture of the network should reflect the organization's needs and resources, and expert assistance may be required to design and implement it. The ISO27033 series of standards, which deal with network security best practice, are also worth reviewing.

The recruitment of an experienced and effective network manager is a key step for the organization. External assistance may be required in the recruitment process. This person's job description should include a clear description of the network(s) for which he or she will be responsible, and the standard to which the network(s) will have to be maintained should be set out explicitly, with objectives and measurable standards of performance. Those aspects of the ISMS for which the job holder will be responsible should also be specifically identified. The job description should contain a clear reference to the job holder's responsibility for maintaining the integrity, availability and confidentiality of data on the assigned network(s).

The network architecture should be specifically documented, including the planned detailed configuration settings of all its hardware and software components. This plan should reflect a risk assessment (as described above) and should be carried out with the assistance of a specialist network engineer. The implementation of the plan should also be in the hands of specialists and, both once it is finished and at periodic intervals thereafter, should be subject to technical audit. Developments in networking technology

should, where appropriate, be integrated into the existing network, subject to normal change management controls.

Security of network services

Control 13.1.2 of ISO27002 says the organization should provide a clear description in its ISMS and in the network services agreement (even where the services are provided internally) of the security attributes (as well as the expected service levels and management requirements) of all the network services it uses. This is referring to the wide range of public or private network services available, which may have simple or complex security characteristics. A clear description of these characteristics should be provided so that appropriate risk assessments can be carried out and so that, when security incidents involving these services take place, adequate information is available to deal with them. Increasingly, the most common source of network service is the internet, and its security characteristics are non-existent.

In addition, as organizations outsource technology and buy other critical services on application service provider (ASP) models, these control requirements become more important. Internet service providers (ISPs), server farms, hosting services, managed service providers, dedicated information services and so on can all provide services that are critical to the security of the organization. It is therefore necessary to identify and document their security characteristics.

Typical network services include: directory services, e-mail, file sharing, instant messaging, printing, file servers, voice over IP, etc.

The network services security characteristics in which the organization should be interested include:

- security technology, such as encryption, authentication and network connection controls;
- the technical parameters for connecting with the service provider securely;
- procedures for restricting access to the services, where necessary; and
- controls relating to any data (particularly personal data) stored on the system.

It is particularly important to check the resilience of the supplier's systems and to understand and check its fall-back procedures. The organization should establish the extent to which the supplier will maintain security

controls when it is in fall-back mode. There should therefore be a risk assessment for every outsourced provider that identifies these sorts of risks and proposes additional controls to offset any observed security weaknesses.

Segregation in networks

Control 13.1.3 of ISO27002 says the organization should introduce controls into its network(s) to segregate groups of information services, users and information systems. As organizations extend their information services beyond the traditional boundaries of the fixed LAN or WAN, so they increasingly need to share information processing and networking facilities. These sorts of extensions increase the risk of an attacker finding a way of accessing facilities or information that is confidential, and therefore some components of networks need protection from other network users. A full risk assessment and cost–benefit analysis (considering also the value of the assets to be secured, and how their interrelationship might need to be safeguarded – segregation, for instance, might reduce the total impact of a service disruption) should be carried out before making a final decision as to how these issues should be tackled, and specialist external advice may be needed to ensure that the choice of technologies and architecture is appropriate to the organization's needs. The existing organizational policies on access control, access requirements and information classification should be cross-referenced in segregating networks.

The creation of demilitarized zones (DMZs) or extranets reflects exactly these needs. Specific resources are gathered together and placed outside the core organizational firewall, and access is then allowed using one or a number of the protocols and technologies discussed earlier in this chapter. Servers operating on the DMZ, outside the corporate firewall, should themselves be configured so that they do not help an attacker find a way past the firewall. For instance, unnecessary services running on these servers, such as FTP (File Transfer Protocol), DNS (Domain Name Service) and SMTP (Simple Mail Transfer Protocol), can leave hackers with ways in. DMZ servers should be precisely configured for their desired role, and no additional services should run; the default set-ups should be modified in the light of a risk assessment.

VLANs (virtual LANs) are logical LANs, based on physical LANs. VLANs use VPN technology to provide logical segregation rather than physical segregation.

Wireless networks should be considered for segregation; the higher level of risks associated with wireless networks might lead a risk assessment to conclude that wireless resources should be networked together and provided with a single secured link to an otherwise secure network. Such a secure link could be through a firewall or other mechanism. There will still need to be a procedure for dealing with rogue wireless access points.

Network architecture of larger, more complex networks might divide the network into a number of logical network domains, with each domain representing differing trust levels (eg desktop access, finance, marketing, etc), each protected by a defined logical security perimeter. This perimeter is created by installing firewalls between the logical domains and interconnecting them in such a way that they control access and information flow between the domains. The fire-walls can be configured to filter traffic in accordance with the risk assessment (one of which should be conducted for each domain) and to block unauthorized access in accordance with the access control policy.

Domains and their relationships should be specifically documented, both on the formal network map and on a schedule that identifies assets and systems and the domains within which they are included. Different parts of a single system (eg an ERP system) could be in different domains; this can be secure if the security architecture keeps the different parts logically separated.

20

Exchanges of information

Control objective A.13.2 exists to prevent loss, modification or misuse of information exchanged either within or between organizations. Such exchanges of information should also comply with any relevant legislation.

Information transfer policies and procedures

Control 13.2.1 of ISO27002 says the organization should put in place formal policies, procedures and controls that protect the exchange of information through the use of any communications facilities, including letter, e-mail, voice, facsimile and video communications facilities. The risks associated with these methods of communication have been discussed earlier in this book and are summarized here. E-mails can go astray or be intercepted and are also a widely used medium for harassment, information leakage, and so on. One could be overheard while talking on a mobile phone in a public place, such as on a train. Answering machines can be overheard by someone physically present in the room as the caller leaves a message. Unauthorized access to dial-in voicemail systems (phone hacking) is a clear danger, as is unauthorized dial-in to teleconferences. Facsimiles and e-mails can accidentally be sent to the wrong destination and the wrong person.

So, information security could be compromised by any of these events. It could also be compromised by the theft or disappearance of critical mobile phones or by the failure of communications facilities (whether through overload, interruption or mechanical failure or even through failure to identify and pay appropriate service provider invoices in due time). Information can also be compromised if unauthorized users can access it. A smartphone with an e-mail box on it exposes potentially confidential information to an attacker; a mobile phone that carries a list of pre-programmed contact telephone numbers can, in the wrong hands, reveal sensitive information.

There should therefore be a clear, formal policy, procedures and controls within the ISMS to protect information exchanges through all possible routes and setting out to employees what is expected of them when using any of these communications methods. These requirements should be part of the training for all staff. Users of mobile phones should receive a mini-restatement of the current version of the procedure when they are issued with corporate mobile phones. Secure use of social media should be covered in staff awareness training.

The measures should include the following:

- There should be procedures designed to protect exchanged information from interception, copying, modification, misrouteing and destruction. Subject to the risk assessment, these are likely to include technological controls such as digital watermarking or encryption and other cryptographic techniques to protect confidentiality, integrity and authenticity, etc. The organization's policy should link the method of protection to the level of classification and should have regard to any applicable legal requirements.
- We have already discussed the need for procedures to protect against malware, and the organizational policy on information exchange should reference the anti-malware policy and controls, just as it should reference the acceptable use policies and the formal guidelines for the retention and disposal of information. Sensitive documents should not be printed to, or left on, widely accessible printers or fax machines. The usual way to deal with this is for there to be a small number of personal (or otherwise supervised), dedicated fax machines and printers to which sensitive information can be printed.
- The dangers of wireless communications should be clearly identified and the policy and controls implemented in this regard clearly referenced in the statement of applicability (SoA).
- The acceptable use policies and any external party agreements for use of the organization's facilities should set out clearly the responsibilities not to compromise the organization through harassment, obscene messages, defamation, impersonation, the forwarding of chain e-mails, unauthorized purchases, etc.
- Remind staff that they should not reveal confidential information when using mobile or fixed phones other than from secure locations. Public places, open offices, offices with thin walls, competitors' premises and

crowded trains are all places from – or to – which confidential information should not be communicated. The best way to do this is to avoid having these sorts of conversations other than from a secure location. In fact, the same rules apply to confidential discussions: they really should only take place in secure rooms that do have soundproofed walls. Subject to the risk assessment, there are many conversations that should not take place until the designated discussion venue has been swept for bugging and other espionage devices.

- Avoid using communications equipment that may be compromised; telephone systems in competitors' premises may be wire-tapped or have conversations otherwise recorded. Many telephone calls to and from investment banks and other institutions are automatically recorded ('for training purposes'). Mobile phones can be hacked and messages intercepted.
- Messages containing sensitive information should not be left on answering machines or voicemail systems where they might be overheard or replayed by unauthorized persons, or the messages re-routed to an inappropriate person or stored in some communal database. It is even possible that a caller might misdial and leave a compromising message on an unknown voicemail system.
- E-mail messages are easily misrouted or intercepted. The three most common problems are, first inadvertently choosing an incorrect recipient from the cached list in Outlook 'To' fields, second, inadvertently including a list of external recipients in the 'copy to' field rather than using 'BCC', and, third, inadvertently replying to 'all' rather than to the original sender alone with information that is intended only for that individual. Those in a position to commit these errors with sensitive information should be trained to review the e-mail addresses in the 'To' and 'Copy to' boxes before they hit 'Send'. Where there is a risk of interception, then e-mail encryption is the only answer. There is some personal data, such as personally identifiable information ('PII') that can legally only be transmitted when encrypted.
- Equally embarrassing can be the dispatch of an electronic document that contains sensitive changes that can easily be revealed to the recipient through Word's 'Show' menu. Sensitive documents should either have all changes accepted prior to dispatch or, better still, should be converted to .pdf format prior to dispatch.

- E-mails are not reviewed and approved before despatch; this means they could provide grounds for legal action in respect of slander, libel, misrepresentation, etc.

Staff training should include awareness of what corporate messaging systems may NOT be used for: anything illegal, potentially damaging to the organization, or which might undermine the credibility or reputation of the organization. There should therefore also be appropriate rules about archiving and storing of electronic messages, so that the organization has vital evidence available to it as and when it might need it.

Bear in mind that most communication channels also provide channels for the unauthorized exfiltration of valuable or sensitive data, and for the import of malware and unauthorized software. The management challenge is to find constructive ways of accessing the communication channel without exposing the organization to unnecessary risks.

Agreements on information transfers

Control 13.2.2 of ISO27002 says the organization should have (primarily) formal agreements for the electronic or manual exchange of information (including personal data) and software between organizations. These might include escrow agreements, which are particularly important where one organization relies on the software developed by another and there is even the slightest chance that the developer might go out of business at some point.

The sensitivity classification of the data to be exchanged should govern the security conditions to be included in the agreement. Where necessary (that is, where there is uncertainty about the appropriate level of protection), a risk assessment should be conducted. The issues that should be addressed in inter-organizational agreements for information exchange do depend on the sensitivity of the information. Information exchange agreements should reference any of the relevant policies and procedures that the organization applies to information exchange and could, according to clause 13.2.2 of ISO27002, include:

- identification of who is responsible for controlling and notifying transmission, dispatch and receipt on either side of the agreement;
- notification procedures to ensure that the other side knows that sensitive information has been dispatched or received, and associated (primarily technical) controls to ensure traceability and non-repudiation;

- minimum technical standards for packaging and transmission;
- courier identification procedures;
- responsibilities and liabilities if data are lost or there are information security incidents;
- the agreed labelling system, to ensure that the appropriate protection required is immediately obvious and provided; the preferred system should (practically) be the same as that used by the receiving organization internally, as this will ensure that there is consistency of understanding;
- where relevant, responsibilities for information and software ownership, and for data protection, software copyright and ownership and similar issues;
- where relevant, technical standards for recording and reading information and software;
- any special controls (such as cryptographic) that may be necessary for particularly sensitive information;
- the concept of a chain of custody is helpful when considering how to safeguard critical information that is being moved between two entities with possible stops en route.

The person(s) responsible within the organization for the maintenance, dispatch and receipt of such information and software should be asked to draft the procedures; it may be necessary after that to ensure that the procedures are made as practical as possible.

E-mail and social media

E-mail is a substantial and fundamentally important subject in the Information Age but electronic communication goes far beyond that. The policy aspects of controls A.13.2.1 and A.13.2.4 have therefore been addressed together in this book, and this next section will cover all the issues surrounding e-mail, social media and their usage.

ISO27002 says the organization should develop and implement a policy, and put in place controls, to reduce the security risks created by e-mail. Obviously, the degree to which these controls will be required will be dictated by the findings of a risk assessment.

E-mail has completely replaced telexes and is well on the way to replacing faxes and traditional, or 'snail', mail. Key differences between e-mail and

snail mail are the speed of the former, its message structure, informality, ease of misdirection, ease of duplication, ease of interception and the ease with which it can carry attachments. This means that there are a number of issues to be considered around the headings of security risk and user policies.

Internet access sits alongside e-mail as an issue that is directly related to the activities of individual employees, and there are similarities between some of the control principles in each area. This chapter therefore also deals with internet acceptable use policies (AUPs).

Security risks in e-mail

ISO27002 identifies a number of security risks in e-mail. These include:

- vulnerability of messages to unauthorized access, to unauthorized modification and to denial-of-service attacks;
- vulnerability of messages to error such as incorrect addressing, misdirection or just the unreliability of the internet;
- issues around instant messaging and file sharing;
- legal issues, such as potential need for proof of origin, dispatch and receipt;
- uncontrolled remote user and internet access to e-mail accounts.

More important than any of these is the risk to the company that e-mail sent between organizations by individual members of staff may lead to unauthorized exposure of confidential or sensitive information and a breach of confidentiality, leading to bad publicity and possibly legal action. There is already case history to show that organizations can be exposed to libel writs as a result of what a staff member has written in an e-mail message, probably informally and for internal distribution only. There is also the requirement for organizations to ensure that confidential information that may affect share prices is not leaked and that Stock Exchange regulations are all observed.

Organizations should draw up clear policies on the use of e-mail. These should be included in the ISMS, and all members of staff should be required, as part of the formal user access statement, to agree to abide by them. The first decision that the organization has to make relates to the private use of e-mail facilities by employees. The fact is that e-mail use is now so ubiquitous that it is virtually impossible to prevent employees from using a work

e-mail facility for private communications; attempts to stop this can be very difficult to enforce and so it is more practical to concentrate on controlling the risks.

An e-mail policy should set out:

- Employee responsibility not to compromise the company, forbidding the use of company e-mail for sending defamatory e-mails, or for harassment, unauthorized purchases or the publishing of views and opinions about suppliers, partners or customers of the organization.
- All e-mails should have an automatic footer that contains the legal disclaimer, with the addition of a statement to the effect that the views expressed in the e-mail are those of the sender alone and do not reflect the views of the organization.
- There may need to be a legal statement in respect of the processing of the recipient's personal data and there may be legal requirements to include company registration information.
- That e-mail is not to be used to communicate sensitive information with specific classifications.
- That e-mail attachments should be appropriately protected, using (where necessary) cryptographic controls of some sort.
- How to respond to viruses and hoax virus messages.
- The incident reporting procedure and the requirement not to pass on hoax virus messages should be included in the e-mail policy.
- A clear procedure around e-mail inbox sizes is required. As e-mail is increasingly recognized as a record of corporate communication and a record of possible wrongdoing, so organizations need to develop methodologies that enable them to manage their e-mail records effectively. These procedures need to be in line with both statutory and regulatory data retention requirements and evidential guidelines. E-mail inbox management procedures that limit mail inbox sizes and encourage employees to destroy e-mails they no longer wish to retain may fall foul of regulatory data retention requirements and run counter to the information security requirement that information be available in line with business requirements. Technological solutions, such as single-instance e-mail storage, are a practical way of dealing intelligently with this challenge.
- That e-mail may not be used to purchase anything on behalf of the organization without specific prior authorization, and then only in accordance with the organization's current policy on purchasing.

- That the corporate e-mail address may not be used for personal purchases or any other personal transactions.

Organizational purchasing policy does need to take into account the ease with which purchases can be made by e-mail and lay down very specific guidelines for staff on this issue. Where e-mail is to be used between organizations as part of the purchasing process, the two organizations should document the basis on which trading will occur and precisely what weight is to be attached to e-mails. For instance, it might need to be agreed in a heads of agreement document that e-mails will not constitute an implied contract between the organizations and require that all contracts continue to be made in writing, signed and sent by post or fax. The passage, in the United Kingdom, of the Companies Act 2006, which made the use of e-mail in the procurement process legal, makes it even more important that these issues are dealt with.

Spam

Spam is a significant e-mail issue. Spam originates outside the organization and exists in such quantity that it can restrict the availability of information, as well as consuming expensive bandwidth. The organization does therefore need to develop appropriate controls to deal with it. These controls need to take into account the possibility that not all spam is genuinely unwanted; some spam is legitimate and useful marketing communication. Moreover, much standard e-commerce information – such as purchase receipts, downloadable documents and other automated services – can be identified as spam by spam filters that are set too widely, and organizations need to consider their information availability requirements alongside their bandwidth and other requirements.

The organization's spam controls therefore need to be a combination of internet gateway restriction (a software or outsourced solution), user training (encompassing both configuration of spam filters, use of white lists and due caution with e-mail addresses) and pressure on the ISP.

Misuse of the internet

There are a number of issues associated with employees surfing the net during work hours and from organizational facilities. Seventy-eight per cent

of respondents to the FBI/CSI 2002 survey detected employee abuse of internet privileges. Each of these issues has implications for the confidentiality, integrity or availability of information.

Employee productivity can be significantly reduced by the time demanded by the wide range of interesting activity, from stock markets to games to chat rooms and Facebook, that is available on the internet. Some research suggests that 30–40 per cent of employee internet activity is not work related. Network traffic can be significantly affected, with resulting reduced business performance, by the combination of recreational surfing by employees and bandwidth-intensive activities such as accessing streaming video and audio, MP3 downloads, image downloads, sharing digital photographs (such as holiday snaps), social networking sites such as Facebook, etc. The bandwidth put in and paid for by the organization is designed for organizational use, not for individual benefit.

As we have already stated, the internet is wild; allowing employee access to the internet allows all sorts of malware to access the organizational system in return. There is a discussion of how an organization's defences can be breached in the section in Chapter 21 on e-commerce security.

Recreational surfing can lead employees to access inappropriate sites, such as pornographic sites (apparently something of the order of 70 per cent of the UK's internet porn traffic occurs between 9 am and 5 pm) and sites promoting violence, discrimination and all sorts of other inappropriate matters. They can also access sites that will download illegal or pirated software, pirated games, pirated videos or pirated music or hacking tools. The organization with the network through which such downloads are made could find itself inadvertently liable for the criminal behaviour of its employees. Free access to the internet can lead to lawsuits, harassment charges (sexual harassment charges can arise from objectionable or sexually explicit material being brought into the workplace by one employee and being seen by another, even where the other person was not meant to see it) and even criminal prosecution (an employee downloading illegal material, or forwarding it from the organization's computers, might create just such a risk).

Clearly, organizations that find themselves forced to dismiss employees for accessing illegal or offensive material can be severely damaged by the resulting negative publicity, not least because the dismissal could in the United Kingdom, under a number of circumstances, be ruled by an industrial tribunal to be 'unfair'.

Organizations should counter these risks by a combination of surf control technology and a well-designed and enforced acceptable use policy (AUP).

Surf control, or filtering, technology is widely available and can be installed both on organizational networks and on individual workstations. The software package should be chosen in the light of the AUP; the AUP should not be built around the limitations of the chosen package. An appropriate package should allow the organization to impose different restrictions at different times of day (eg possibly slightly more lenient outside normal work hours) and for different user groups (eg possibly slightly more lenient for senior managers or research staff). It should allow blocking of specific sites, as well as broader categories or groups of sites, so that restrictions can be focused in the light of business needs, rather than over-blocking in a way that goes against business needs.

The package should also work effectively across the entire inbound and outbound communication channel. It should be capable of applying the organization's selected security controls to e-mail, instant messaging, Internet Relay Chat, chat boards and blog sites, Facebook, peer-to-peer networking and other social media sites.

The package's reporting tools should enable the organization to know when and how many unauthorized site access attempts there are, and by whom, so that the individual concerned can be helped to comply. The package must be interoperable with the organization's chosen firewall. It must provide centralized, scalable control so that it can support a growing organization. It must also be capable of handling daily updates, so that newly identified unacceptable websites can be easily barred.

While there is further discussion of the legal issues surrounding data security later in this book (and readers should refer to it, as well as to their professional advisers, for additional information), it is appropriate at this point to state that an AUP that will comply with the relevant legislation must:

- be in writing;
- be clearly communicated to all employees;
- set out permissible use of both internet and e-mail – eg for business purposes only;
- specify what uses are prohibited – eg downloading offensive, pornographic or illegal material;
- state what monitoring (if any) will take place;
- set out acceptable online behaviours;
- specify which online areas are prohibited – eg pornographic or hate sites;

- set out privacy rules in relation to other users, and in respect of the employer's right to monitor the employees' activity;
- set out the likely disciplinary consequences of breaching the AUP.

One site worth visiting for more information is: www.iwf.org.uk (archived at https://perma.cc/VUM2-HCZB), which is the site of the Internet Watch Foundation, set up in 1996 by UK internet service providers (ISPs) to tackle criminal content on the internet, to provide a hotline for reporting illegal content and to advise internet users on how to restrict access to harmful or offensive content.

Internet acceptable use policy

An internet AUP should combine statements on use of the internet and use of e-mail. E-mail issues were addressed earlier in this chapter. Variations to what is set out below will depend on the conclusion that the organization reaches regarding private usage of its internet facilities; this statement reflects a far-reaching restriction, and not all employers will consider all its components necessary. It is important that, as for all other components of the ISMS, the organization adopts and develops an AUP that reflects in detail the culture of the organization but that also provides the level of security required by a risk assessment:

- General statement: this should start off with a reminder about the dangers of the internet and say that the company will not be liable for any material viewed or downloaded. It should continue by saying that use of the internet must be consistent with the organization's standards of business conduct and must occur as part of the normal execution of the employee's job responsibilities. Any breach of the AUP may lead to disciplinary action and possibly termination of employment. Illegal activities may also be reported to the appropriate authorities.
- Organizational user IDs or websites (or e-mail accounts) should only be used for organizationally sanctioned communication.
- Use of internet, intranet, e-mail and instant messaging may be subject to monitoring for reasons of security and/or network management and users may have their usage of these resources subjected to limitations.
- The distribution of any information through the internet (including by e-mail, instant messaging systems and any other computer-based systems)

may be scrutinized by the organization, and the organization reserves the right to determine the suitability of the information.

- The use of organizational computer resources is subject to (English or Scottish) law and any abuse will be dealt with appropriately.
- Users shall not visit internet sites that contain obscene, hateful or other objectionable material, shall not attempt to bypass organizational surf control technology and shall not make or post indecent remarks, proposals or materials on the internet.
- Users shall not solicit e-mails that are unrelated to business activity or that are for personal gain, shall not send or receive any material that is obscene or defamatory or that is intended to annoy, harass or intimidate another person, and shall not present personal opinions as those of the company.
- Users may not upload, download or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties, may not reveal or publicize confidential information (refer explicitly to the information classification levels selected by the organization) and shall not send confidential e-mails without the level of encryption required in terms of the specified policy in the ISMS.
- Users shall not seek to avoid and shall uphold all malware prevention policies of the organization, shall not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and shall not examine, change or use another person's files or any other information asset unless they have explicit permission.
- Users shall not carry out any other inappropriate activity as identified from time to time by the organization and shall not waste time or resources on non-company business. This includes downloading from social networking sites, bandwidth-intensive content such as streaming video and MP3 music files, sharing digital photographs, etc.

The AUP should, if possible, be developed in a way that involves staff from within the organization; certainly, all staff will need to be trained to ensure that it is understood. The training activity should be detailed and ongoing and should include notifying employees of changes to the policy and its implementation. All employees should accept the AUP at the time that they sign the user access statement (control A.8.1.3). Copies of the AUP should also be prominently posted in any employee resource centre or staff internet

cafe from where activity to which the AUP applies will take place. Of course, the right filtering software, properly installed and dynamically managed, should help the organization avoid needing to take disciplinary action in respect of employee behaviour on the web.

Social media

Facebook, LinkedIn, Instagram, Twitter and YouTube are the world's most popular sites for people to share information, socialize and just hang out together, electronically. Blogging, instant messaging and Skype all play a significant role in enabling people to keep in touch with one another, wherever they are in the world.

Collectively, sites and internet services like these are known as social media. How should organizations regulate and manage the use, by their staff, of social media during work hours? What sort of risks do organizations face, in terms of potential data loss, unregulated communication of confidential information and loss of work time? Answering these questions – assessing and controlling the new risks associated with the use of social media – should be addressed as part of the ISMS. Even more than mobile communications and the 'porous perimeter' created by the proliferation of laptops, mobile phones, social media make individuals – potentially every individual within the organization – a critical point of presence for organizations on the internet. Smartphones increasingly have social media applications available on the mobile platform. Some organizations recognize risks to their information by denying the social media revolution and banning access to social media sites during work hours. Their marketing and communications teams have limited, if any, access to these channels. Sales teams that ask for instant messaging services are denied.

Other organizations recognize that social media are just another communications medium and develop an appropriate social media strategy. These organizations:

- identify their corporate social media objectives;
- do a risk assessment (threats, vulnerabilities, likelihoods, impacts);
- assign roles and responsibilities;
- develop a social media policy and an appropriate mix of procedures and guidelines;

- acquire the appropriate technical controls;
- train staff on how to behave and what to do;
- implement a monitoring and review framework;
- make social media a regular part of how they do business.

In other words, they tackle social media activity as a key part of their overall ISMS. The specific ISMS control areas that should include aspects of social media are policy, roles and responsibilities, AUP, account management, classification, anti-malware, back-up, incident management, monitoring security, privacy, and terms and conditions.

21

System acquisition, development and maintenance

Control category A.14 is there to ensure that security is built into information systems as an integral part. Systems, in this context, include infrastructure, external systems, commercial off-the-shelf (COTS) packages, operating systems, business applications and user-developed systems. How the business process that will support the application or service is designed and implemented will critically affect its security. Therefore, security requirements should be identified at the requirements-gathering stage of the project and justified, documented and built into the system from the outset. This is an area in which the organization is likely to need specialist external advice unless it already has the expertise in-house.

Security requirements analysis and specification

Control 14.1.1 of ISO27002 says the organization should specify, in the business requirement document for a new system or in that for an enhancement to an existing system, the requirement for controls. Identifying policy and compliance requirements, threat modelling and incident analysis should all contribute to the identification of security requirements for new systems. Security vulnerabilities should be recognized from the outset (through a risk assessment), and the security requirements (including the need for fall-back arrangements) should be developed alongside the functional requirements. Any procedures that the organization has for system requirements analysis should include reference to security analysis to ensure that it is tackled from the outset, rather than as an add-on. Controls identified and implemented at the outset are much less expensive to implement and maintain, and often more effective than ones developed and implemented later.

These specifications should consider automated controls to be included in the system and should also consider the need for any supporting manual controls. Similar considerations should apply when considering third-party software applications. As usual, the measures implemented should reflect the business value of the information being protected and could therefore include specific requirements such as:

- the reliability of user authentication;
- how access provisioning for users, system administrators and privileged users will fit within the organization's existing requirements in these areas;
- how confidentiality, integrity and availability of affected assets might be affected;
- requirements in terms of transaction logging, monitoring and non-repudiation;
- interfaces with other security requirements and processes.

It might be appropriate for the organization to adopt a policy that it will use only third-party products that have been independently assessed and certified and that meet minimum security standards. Certainly, there should be a formal process for testing COTS products, and contracts should only be finalized once they can include appropriate requirements for addressing any security issues that have been identified. Where the supplier cannot meet the requirement, alternative controls should be considered such that the criteria for the organization's risk treatment plan can be met. If a product provides unwanted security features, they should either be disabled or incorporated into the existing framework if there is a way in which this can cost-effectively enhance organizational information security.

Securing application services on public networks

Control 14.1.2 of ISO27002 focuses on the need to ensure that information used in applications or application services and which passes over public networks should be protected from fraud, contract dispute, and compromises to its integrity and confidentiality.

As online commerce has become more and more widespread, so a control category that dealt primarily with e-commerce has been expanded to deal

with security in a wide range of application activity on the internet, including application-based e-commerce.

Control A.14.1.3 now requires any organization involved in 'application services transactions' (which includes traditional e-commerce and in-app transactions) to protect that information and its services against fraudulent activity, contract dispute, disclosure or modification of information, misrouting of information, unauthorized duplication and incomplete transmission.

This is also an area of considerable interest to credit card payment providers and to banks. The Payment Card Industry Data Security Standard (PCI DSS) (for more information, see www.itgovernance.co.uk/pci_dss (archived at https://perma.cc/6P4T-G3JP)) is significantly important to all e-commerce merchants and intersects with the requirements of ISO27001.

E-commerce issues

E-commerce can involve electronic data interchange (EDI) as well as e-mail; however, it is now primarily web-based trading and online transactions. There are a number of issues that need to be tackled, with controls introduced; web transactions take place within a rapidly changing environment in which some fundamental security principles have emerged. There are also specific issues that need to be considered in the use of extranets by businesses in trading with supply chain partners.

The e-commerce world is changing rapidly. This has immediate and constantly changing implications for information security. Organizations are changing, becoming more open; they are also becoming more complex. As companies acquire others, or develop business partnerships, so they want to share information across spaces that are no longer strictly limited to an organizational domain. The drive towards more open business models is driving forward greater interconnection and greater sharing of information. Technology is contributing to these changes, as more and more powerful applications are developed to push information around the world and to overcome any barriers in its way. Content is no longer limited to text; it now includes documents and active content (mobile code, such as Java or ActiveX) that download and run on users' desktops; it includes voice, sound, animation, streaming video, instant messaging, file transfers and a whole range of multimedia applications. All these changes help the development of e-commerce, so organizations, and users within them, want to respond to

and use all the new capabilities. These changes also create a whole new and fast-changing series of risks and vulnerabilities and a very porous organizational security perimeter.

Technology changes are at the heart of these changing threats. Applications are increasingly written to assume that information will be shared across networks, regardless of the organizational boundaries or firewalls between them. Many vendors are now actually building their applications to overcome or circumvent the firewall controls, which are often viewed as barriers to e-commerce, barriers that must be overcome in the pursuit of open, networked working. One ongoing change is that increasing numbers of internet application developers are making new applications run via the firewall port that is mostly open (port 80, traditionally enabled on 99.9 per cent of firewalls to run HTTP). This means that a diversity of media types try to navigate port 80, making it difficult for firewalls to filter out malware or to control access to specific data channels. Of course, as new applications are developed and firewalls lag behind in their ability to handle the new application effectively, so organizations will take increasing risks by opening their firewalls anyway – particularly where the application is considered critical to the business.

The risk from hackers is growing all the time. There was a detailed discussion of the world of hackers in the context of access control, and this is also highly relevant to the consideration of e-commerce. Organized crime, as was described in Chapter 1, is turning to the internet and e-commerce as a lucrative business area, the growth of phishing, pharming, website drive-by attacks and increasingly sophisticated spam mail are some of the most visible and high-profile indicators of the extent to which e-commerce is also a danger area for consumers and businesses. Equally important are the risks arising from industrial espionage and the value that transactional information can have to a competitor, even if it has only been inadvertently disclosed.

Non-repudiation is a major issue for online commerce. As commercial transactions take place over the internet, the same types of dispute that arise in the analogue world arise in the digital one. Disputes can involve the specifics of agreements and performance, and there are digital equivalents of the postmarks, recorded delivery receipts and notarized documents that exist in the analogue world. There are three key components to the non-repudiation issue:

- *Non-repudiation of origin.* There must be evidence for a receiving party that the sender is genuine, not an impostor. A vendor would, for instance, want to be sure that an order was from a genuine customer.

- *Non-repudiation of submission*. There must be evidence (such as a postmark) that the thing was actually sent at a particular time.
- *Non-repudiation of receipt*. It must be possible to prove that the receiving party has actually received what was sent. Lesser issues include verifying the time and place of transmission.

Application Service Management is an emerging discipline that deals with how transaction information is delivered to an end user through an aggregation of interdependent applications, operating systems, hardware platforms, and network connections; it recognizes that effective e-commerce depends on much more than simple transaction-level security.

It is against this background that the issues identified in clause 14.1.3 of ISO27002 should be considered. The control objective is that application services information passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. In implementing this, there are a number of interlinked issues, many of which should be addressed in formal agreements between parties:

- Authentication, to ensure that there is some confidence that customers or traders are who they say they are.
- Authorization, to ensure that trading partners know that prices set, or contracts agreed, have been agreed by someone authorized to do so, and that trading partners know what each other's authorization procedures are.
- Dealing, in online contract and tendering processes, with non-repudiation, with confidentiality, integrity, proof of despatch and receipt of documents.
- How confidential are discount arrangements and how reliable are advertised prices?
- How is the confidentiality of transaction details (including payment and delivery details) to be protected?
- What vetting of payment information is necessary?
- What is the most secure method of payment, and how is credit card fraud to be dealt with?
- How are duplicate transactions, or loss of transactions, to be avoided?
- Who carries the risk in any fraudulent transactions, and how is insurance to be dealt with?

As can be seen, these questions and the controls they should instigate are specifically designed for business-to-business (b2b) commerce; trading

partners should incorporate their answers to these questions into an agreement between them. Trading partners operating through an internet exchange or via an extranet also need to resolve these issues. Many, but not all, of the issues listed above can be solved by implementing effective cryptographic controls. Cryptographic controls, encryption, digital signatures, non-repudiation services and key management are the subjects of control 10.1 of ISO27002.

These controls need to be extended to cover business-to-consumer (b2c) commerce for all organizations that sell via the web, particularly in respect of the implications of data protection legislation, phishing attacks and credit card fraud. The organization also needs to determine which laws and jurisdiction apply to which transactions.

Security technologies

The speed of change, the range of threats and the variety of technology available mean that it is virtually impossible for an organization's information security specialist, let alone the business manager responsible for information security, to be adequately informed on the subject. It is essential that any organization implementing web-based services take professional advice from a security organization that is technology agnostic and that can provide completely up-to-the-minute advice on appropriate technology steps. In assessing an adviser, consideration should be given to its financial and business viability in the same way as the creditworthiness of a potential client might be assessed. This is trebly important for any potential supplier of security technology; not only does one need to have some certainty that the company will survive to service and develop its technology, but there also needs to be some certainty that the technology itself is, or will really be, part of the mainstream.

The Internet Engineering Task Force (IETF) is an open, international community of practitioners concerned with the evolution of internet architecture and its smooth operation. It has a number of working groups, which consider and propose official standards and protocols for use on the internet. Its website can be accessed at www.ietf.org (archived at https://perma.cc/WQ56-M5UM). The fact that a protocol has been adopted by the IETF and by a number of supporting organizations does not, however, mean that every single organization in that space has to – or indeed will – use it. The internet is still wild. The four key security technologies (SSL, IPSec, S/MIME

and PKIX) are briefly described below. There are a number of other technologies, with various derivations, but these four are still the technological basis of most internet security systems.

Secure sockets layer (SSL)

SSL is a handshake protocol that was developed by Netscape Communications to provide security and privacy to internet transactions. It is application independent; after an SSL session starts, other protocols (such as HTTP and FTP) can be layered transparently on top of it. It has become one of the most popular security protocols on the internet. Installation of a server ID, or digital certificate, will automatically activate SSL on the server, and this enables that website to communicate securely with any visitor using Microsoft Internet Explorer or any other reputable browser. Client and vendor servers are able to authenticate one another automatically. Once this is complete, SSL will encrypt all communication (data such as credit card numbers and other personal information) between the web server and the visiting browser with a unique session key. The session key is not used again. SSL was designed to ensure that even if information was intercepted, it could not be viewed by someone who was not authorized to view it. SSL3.0/TLS is however vulnerable to an exploit called 'Poodle' and organizations deploying SSL should take expert technical advice in order to minimize their exposure.

Then there is Achilles, a tool available to all on the internet, which can intercept http and https data (by acting as a proxy sitting between a browser and a server) and potentially allow an attacker to alter those data before sending them on. SSL cannot be relied on in isolation; these sorts of 'web application session tracking attacks' are constantly evolving and the organization's defences have to evolve equally quickly. Cookies, which are the most widely used session tracking mechanisms, and which are stored in the browser, can be edited in such a way that the attacker can usurp another user's session on, for instance, an e-bank site. The organization's information security adviser and specialist technology advisers should (assuming that the risk assessment identifies this as an issue) take steps to ensure that the security of the session tracking mechanisms of web applications is assessed and any weaknesses repaired before an attacker takes advantage of them.

The default settings on Microsoft and other reputable browsers should show the user a warning that the site to which information is about to be

submitted is insecure, that the communication could be observed by a third party and that passwords, credit card numbers or other confidential information should not be submitted. The warning does not appear where there is a valid SSL connection. There are other signs that there is an SSL connection: the URL prefix will change from http to https and a closed padlock will appear in the bar at the bottom of the browser window.

Internet Protocol Security (IPSec)

Where SSL allows two systems to communicate securely over an insecure connection, IPSec creates a secured connection between the two systems. IPSec defines how interoperable, secure host-to-host and client-to-host connections (known as virtual private networks, VPNs) are to work, creating an encrypted tunnel over a public network that provides privacy as good as that available on a private network.

S/MIME

Multipurpose Internet Mail Extensions (MIME) is a specification that provides a standard method for attaching to basic e-mail messages additional files such as pictures, audio and application files. Secure MIME (S/MIME) adds security features such as digital signatures and encryption services to the basic MIME specification, thus protecting the privacy of e-mail and its attachments. S/MIME provides authentication, message integrity and non-repudiation of origin (using digital signatures), and privacy and data security (using encryption) for e-mail, and is built into most modern e-mail systems.

PKIX

The PKIX working group of IETF has been taking forward work on the definition of a standard, interoperable public key infrastructure and on fostering usage of public key security services. It has specified the mechanisms for encryption and described the structures of public and private keys, certificates and digital signatures. It has also addressed how certificates should be managed, hosts addressed, certificate authorities (CAs) run, and so on. Much more information is available from the IETF website (https://datatracker.ietf.org (archived at https://perma.cc/YSA9-HZVD)).

In addition, and of particular relevance for e-commerce trading, there is the SET (Secure Electronic Transaction) protocol, developed jointly by Visa and MasterCard as a method for enabling secure, cost-effective bank and credit card transactions over open networks. SET includes protocols for purchasing goods and services electronically, for authorizing payments and for requesting and obtaining digital certificates. SET is not, however, widely used, as it requires both customer and merchant to register in advance with a 'payment gateway'. Visa and MasterCard have therefore introduced a new security technology that is easier for customers to use to authenticate themselves, called 3-D Secure.

Server security

Control A.14.1.2 requires the organization to protect itself against modification of information. This points to the need for organizations to take specific steps to protect their web servers from attack. There are a number of baseline security measures that the ISMS should require to be carried out regularly, which should be documented. These are particularly important for (but not restricted to) organizations that run Windows Servers. All browsers have significant vulnerabilities, and users should ensure that they are always using the most recent version of whichever is their preferred browser, with the most recent service pack, or an alternative, demonstrably less vulnerable browser. It would make sense for there to be a specific risk assessment of browsers and for the organization to document a policy as a result of it.

In the context of a Microsoft (or any other server) system, baseline measures should include the following:

- Someone should be appointed to be specifically responsible for the security of the web servers. This person should have adequate specialist training and should have available a completely up-to-date source of information about vulnerabilities, threats, attacks and defences.
- The organization should run the most recent Windows server and browser.
- The more recent the version, the fewer the security-related bugs.
- The organization should install the latest service pack (SP) on each Windows host that houses each Windows server. Service packs are

available, free, over the web from https://www.microsoft.com/en-us/download (archived at https://perma.cc/D8TF-Z6S3).

- The organization should install the latest hotfixes as soon as they become available. These are usually also available directly from the Microsoft website.
- The organization should avoid installing a Windows server on the same physical platform as a domain controller.
- The organization should obtain and apply specialist technical advice on the secure configuration of Windows servers, to at least the level identified in the Microsoft 'Securing your web server' checklist.
- The organization should ensure that the Windows host itself is correctly configured and patched so that any operating system vulnerabilities cannot be exploited to access the web servers.
- Use the CIS benchmarks (www.cisecurity.org (archived at https://perma.cc/F7P2-AKGM)), which run through a downloadable 'Security Scoring Tool', to ensure that their actual configuration meets the industry consensus security benchmarks.

The PCI DSS is particularly concerned about the vulnerability of web servers to external attack. Any e-commerce organization should, as a matter of course, obtain a copy of the PCI DSS (download via www.itgovernance.co.uk/pci_dss (archived at https://perma.cc/6P4T-G3JP)). Two key controls that it mandates are, first, that web server vulnerabilities must be identified and patched, and, second, that the website itself should be subject to regular penetration testing by approved penetration testing companies.

Server virtualization

Server virtualization brings significant cost savings to organizations, with parallel reductions in carbon footprint and other running costs. A server virtualization project may also be accompanied by information security risks, all of which are recognized in 14.1.2 of ISO27002, and the most significant ones of which were identified by Gartner as follows:

- There's usually no risk assessment – IT technicians like to believe there are no risks to virtualization.
- Compromise of the virtualization layer could lead to compromise of all the hosted workloads.

- Communication between virtual machines can take place without the level of monitoring or intrusion detection that might take place on physical networks.
- Workloads of differing trust levels could be consolidated onto the same server without adequate separation.
- Administrative access to the Hypervisor/VMM layer may be inadequately controlled.
- Breach of access controls and desegregation of duties may break down as users and administrators gain access to resources to which they are not entitled.

Protecting application services transactions

Control 14.1.3 of ISO27002 deals with online transactions. The standard seeks the same outcomes that any online customer, credit card company or supplier wants: online information to be protected so that it remains authentic, is complete, is not misrouted, altered, disclosed or duplicated and, in particular, is not stolen so that it can be used in a fraudulent transaction elsewhere. The PCI DSS is particularly concerned about the potential misappropriation of cardholder information, and mandates a number of controls around non-recording and non-storage of sensitive cardholder information such as credit card numbers, authorization codes, passwords, and so on.

The options that ISO27002 suggests should be considered, subject to the risk and cost–benefit assessments, include the following:

- Electronic signatures may be required. These are not always practical for consumer transactions, as so many consumers have not set up digital signatures; they are more appropriate for commercial transactions.
- Technical measures should be considered. They are needed to verify user credentials, including requests for random components of (strong) passwords, to keep the transaction confidential (using SSL technology) and to protect privacy (in line with the privacy policy, which should be displayed on the website).
- The encryption of communications should be explored, whether using the encryption technologies available inside the Microsoft Windows package (in the e-mail Tools/Security menu) or a commercial encryption technology such as PGP (Pretty Good Privacy).

- Personal information storage should not be accessible from the internet; that is, it should be stored on a secure server within the organizational perimeter.
- Security should be embedded end-to-end in a trusted authority relationship.
- Legal issues must be carefully considered: in which jurisdiction does the transaction occur and what legal arrangements must therefore be made to protect it legally? This issue needs professional legal advice.

ISO27002 does not deal with online fraud or phishing attacks but, clearly, any organization (particularly a financial one) that operates a high-volume website must be prone to such an attack. Such organizations need, as a matter of course, to warn their customers about non-disclosure of passwords and to have a fast response mechanism for identifying fraudulent sites and reporting them to their ISP, so that they can be taken down.

22

Development and support processes

The object control category 14.2 is to ensure the inclusion of information security within the development lifecycle.

The Systems Development Lifecycle (SDLC) – also sometimes called the application development lifecycle – is a process for planning, creating, testing and deploying an information system. The term is used to describe whatever mix of hardware, software, coding and application services are required to deliver the information systems objective. NIST has a useful paper on the SDLC at https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final (archived at https://perma.cc/U73D-6BA4). SDLC can operate within any project management environment, from Agile to Waterfall, and with any project management methodology, from Scrum to PRINCE2. ISO27002 provides, in 14.1, a set of relevant controls for system acquisition; the set of controls in 14.2 apply to the systems development activity.

Secure development policy

Technology changes over the last decade have shifted the security focus from the network perimeter (although this still remains very important) toward application security in relation to web-based attacks. Malicious code can bypass firewalls and intrusion detection systems and, as a result, attackers look for opportunities to exploit code-related security vulnerabilities. Some of the most common vulnerabilities (drawn from the OWASP Top 10), which originate in inadequately secure coding practices, include:

- cross-site scripting (CSS);
- SQL injection;
- broken authentication and session management;

- insecure direct object reference;
- security misconfiguration.

As the OWASP websites says: 'adopting the OWASP Top Ten is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.' It is also the logical starting point for the creation of a secure development policy.

Control 14.2.1 identifies a number of issues that should be considered within a secure application development policy, ranging from dealing with security at all aspects of the SDLC through to the adoption of secure coding practices. The key components of a secure development policy might be to set the objective of avoiding any of the OWASP Top Ten vulnerabilities, the adoption of secure coding standards (and the CERT website, at https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards (archived at https://perma.cc/9JGV-V27L)) provides access to secure coding standards for C, C++, Perl, Java and Android as well as its Top 10 Secure Coding Practices and the Secure Coding Style Sheet. Of course, secure coding practices require appropriately competent and trained developers, working in a secure development environment, with a secure development process that includes requirements analysis, security checkpoints, code review, effective version control, and secure repositories.

Logically, if you outsource software development, you might mandate these standards for any of your outsource suppliers.

System change control procedures

Control 14.2.2 of ISO27002 says the organization should strictly control the implementation of changes within the systems development lifecycle by the use of formal change control procedures to minimize the potential for the corrupting of information systems. All changes to systems, even properly authorized ones, can damage the system, with resulting loss of integrity, availability and confidentiality. Application and operational change procedures should be integrated, for the sake of simplicity. Risk assessment, analysis of the impact of the proposed changes and identification and specification of new or amended security controls should be part of this process. The measures that ISO27002 recommends be considered for inclusion in this procedure, which might use a standard form with space for ticking boxes or inserting additional information as necessary, are listed below. In an ITIL environment, this process should be integrated with the CAB

process. These could also be part of any existing formal project management procedure (eg based around PRINCE2):

- There should be a central record of approved authorization levels, which is kept up to date for leavers and joiners, or changes to authority levels.
- Proposals for changes to systems should only be submitted through a centralized scheme by authorized users of the systems, and there should be an audit trail of change requests, indicating what decision was made for each, and why.
- Existing controls and procedures should be regularly reviewed to ensure that they will not be compromised by the proposed changes.
- All computer software, hardware, information assets and database entries that may need to be amended as a result of the change should be identified.
- There should be formal approval of the change before work begins, and this approval should probably be from a line manager, to show evidence that there is a business need for it, and from the information security adviser, to show evidence that all the security issues have been risk-assessed and resolved. There may also need to be technical approval to show evidence that the change, or the new software, will run on the existing system and with the other software deployed on the network. Significant changes should be authorized by an entity such as the information security management forum or the IT governance committee.
- Code changes to sensitive applications should be checked by a second person. This could be required on something as simple as a set of changes to accounting or project codes as well as on more complex applications.
- The implementation should be carried out in a way and at a time that minimizes business disruption and does not disturb the business processes.
- System documentation and user procedures should be updated as soon as the change has been implemented, and the completion of this step should be identified on the approval form.
- There should be some form of version control for all updates (using the vendor numbering system for vendor software updates), and this should be logged on a central register.
- An easy way back to the pre-change status quo (perhaps through the most recent back-ups, or through the existing disaster recovery procedure) should be identified prior to any change being implemented, and a process should be defined to identify and correct any errors, or lost work that may have resulted from a failed change.

Technical review of applications after operating platform changes

Control A.14.2.3 requires the organization to review and test (business-critical) application systems when changes occur. As stated in the subsection above on change control procedures, technical approval for changes might also be necessary. ISO27002 recognizes that this is to ensure that there will be no adverse impacts on system security or operation. Testing of the systems may be necessary to ensure that this is the case. The budget and maintenance plan may need to be amended to take these changes into account, and business continuity plans may also need to be updated.

Restrictions on changes to software packages

Control 14.2.4 of ISO27002 says the organization should discourage modifications to COTS software packages, or, where these appear absolutely necessary, to control them strictly. It is usually better, and generally more cost-effective, for the organization to change its operating procedures to accommodate the software package than to seek to change the software package to suit its procedures. Software packages are increasingly complex, and the skills to modify them are generally native to the vendor. Where, for some business-critical reason, the organization is unable to find any solution other than to try to change a software package, ISO27002 recommends that a risk assessment should first be carried out that identifies, among other things:

- what the risk may be of compromising vendor-designed and in-built controls and integrity processes;
- whether or not the consent of the vendor must be obtained;
- the possibility of the desired change appearing from the vendor at some point as a standard program update (in which case, membership of a product vendor group and pressure on the vendor may be the best course of action);
- the problems that there might be around future upgrades and maintenance if the changes go ahead and the vendor will not support the changes.

Where changes do go ahead (after initiating the change management process discussed above), retain a copy of the original, unchanged software; fully test and document the changes; and ensure that they can be reapplied after all future upgrades. Better still, adapt to the software!

Secure systems engineering principles

Control 14.2.5 says the organization should – particularly if it engages in complex system development – establish clear, documented principles for engineering secure systems and should then ensure these principles are applied to all systems engineering efforts.

Systems engineering is a formal discipline which focuses on how to design and manage complex systems across their lifecycles. System development, design, implementation, and ultimate decommission become increasingly difficult with large or complex projects. A complex systems engineering project, in a large organization, will consider the role of users, the input of stakeholders and the aims and objectives of the system itself; the Systems Development Lifecycle is one of the tools that might be used to engineer a complex system.

For Control 14.2.5, however, secure systems engineering is more prosaically about ensuring that security is designed into all the layers (business, data, applications and technology infrastructure) of a complex information system, and that an appropriate balance – depending on risk assessment and risk appetite – is struck between confidentiality, integrity and availability.

The control guidance says that secure engineering techniques can help with authentication methods, secure session control and data validation, sanitisation and elimination of debugging codes.

Secure development environment

Environments are controlled areas where developers can work on each of the stages of the SDLC. Typically, developers work on their own in a development environment, work can then be merged in a common development environment, basic testing takes place in a systems testing environment, user acceptance testing in the UAT environment and, finally, the software goes into the production environment.

This control which is A.14.2.6, works alongside A.12.1.4, which says these environments should be separate. Separate environments will not bring security benefits if they are insecure; there are therefore a number of considerations which the software development organization might, depending on its risk assessment and the sensitivity of data involved, consider putting in place:

- separation between development environments, depending on the sensitivities of the project;

- physical and logical access control to the development environment;
- managing and monitoring codes changes and code version control;
- controls over data being checked into and out of the development environment;
- security screening of personnel involved in the development activity;
- regular back-ups of the environment, but stored elsewhere and with different access restrictions.

Outsourced development

Control 14.2.7 of ISO27002 says the organization should apply controls that will make outsourced system development secure. Where the organization cannot help itself by using vendor-developed software and must have its own developed, there are a number of measures that ISO27002 recommends it should introduce to try to protect itself during a process over which it has little direct control.

The issues that it must consider, only some of which can be incorporated into a contract (others will require expert supervision that the organization might not have in-house), are as follows:

- licensing, code ownership and intellectual property rights;
- certification (possibly by a third party) of the quality and accuracy (code review) of the work done;
- escrow arrangements (particularly for the source code) in the event of the developer's financial failure;
- rights of access for audit of the quality and accuracy (code review) of the work;
- contractual requirements for code quality, security, and testing;
- pre-installation acceptance testing for Trojans and other malicious code, and to confirm accuracy and correctness of the deliverables;
- quality and accuracy of documentation, including that which describes what has been built;
- delivery dates, change management control and budgetary control.

Security and acceptance testing

System security testing (control A.14.2.8) should take place during each of the development phases. Security testing should be structured and planned,

with clearly determined inputs and expected outputs. An audit trail of testing results, as well as remediation activity, are core components of an effective security testing regime.

The whole point of system acceptance testing (control A.14.2.9) – carried out by the customer – is to ensure that the system meets the original requirements and that, from a security perspective, it won't introduce security issues into the operational environment. This does mean that it should be tested in an environment which is as close as possible to the operational one; it also means that deployment of automated tools and vulnerability scanners could form part of the testing strategy.

While control 14.2.9 of ISO27002 is a short clause – it says the organization should establish acceptance criteria for new information systems, for upgrades and for new versions, and to carry out appropriate tests prior to acceptance – it has a number of implications. This is a clause that is more important for an organization that uses bespoke software or relies on a third party (or internal supplier) to deliver a large IT project than for an organization that uses commercial off-the-shelf software. Nevertheless, it is important, even for such an organization, to establish the basis on which it will accept upgrades and new versions. The key requirement must be that the acceptance criteria for new systems should be clearly identified, agreed and documented. There should be a significant element of user testing against these criteria, which should be clearly related to the requirements specification that was used in initiating the project. The acceptance criteria must be capable of objective and, if necessary, independent testing to determine whether or not they have been met. There should be a formal acceptance process for new software, once it is said to have met its acceptance criteria; this process should involve management authorization.

All off-the-shelf packages have regular upgrades, and Microsoft tends to issue new versions of its software every few years, service packs on a regular basis and patches monthly. A number of other major suppliers have adopted similar upgrade delivery profiles. One issue that needs to be resolved is that of when upgrades or new versions will be deployed. Many IT managers take the view that it is safer to upgrade to a new version (particularly of a Microsoft package) only after it has had a period in the marketplace during which its initial set of bugs can be diagnosed and fixed. Others take the view that the faster the upgrade is implemented, the sooner the organization will be able to have in place software without the known security weaknesses of earlier versions. Of course, it will soon have its own vulnerabilities exposed!

Our view is that users of commercial off-the-shelf software packages should subscribe to the websites of all their software suppliers, should be

aware of upgrades, patches and fixes as they become available and of any new weaknesses or flaws that implementation of the upgrades might cause, and unless they can identify compelling data security reasons not to, should upgrade at the earliest opportunity. Microsoft service packs should be installed virtually as soon as they are available (unless there are compelling reasons not to) through the organization's current change control procedure, and regular upgrades (now usually monthly) from security software providers should also be accepted, on the same basis, as soon as they are available.

Networks running non-Microsoft applications (eg ERP software) should confirm with their vendor that the upgrade will not negatively impact the software. If there is any doubt, a test upgrade in an isolated environment should be performed before the live system itself is upgraded.

Fixes and patches tend to have little or no impact on users, other than to continue securing their information. Across the web, they are usually free. However, version upgrades, other than to antivirus software, may have significant user impacts, and there are usually cost implications. There are a number of controls that should therefore be considered. The first is budgetary. The organization should ensure that it has sufficient budgetary provision to deal with upgrades planned by software vendors. Strategically, it is sensible for organizations to move relatively soon after the issue of an upgrade to its implementation, as the weight of developer resource and support tends to shift away from older packages towards new ones over time, and eventually support for older versions tends to be withdrawn. There are also likely to be compatibility issues between organizations that are using significantly different releases of the same software. There should also be competitive advantage for organizations in upgrading, in that it enables staff to increase their productivity. Users should also be involved early in any upgrade process, to ensure that their needs and wants are identified and, if possible, accommodated.

All these factors should be taken into account in deciding whether or not to upgrade. There may well be hardware or capacity issues (and, therefore, further budgetary issues) that arise from a decision to upgrade a software package, and these need to be considered and taken into account as part of the decision-making process.

Once budgetary issues, user requirements and hardware implications have been accounted for, then assuming that the decision (which should be made through the information security management forum) to upgrade has been made, there are a number of measures that should be implemented.

Clause 14.2.9 of ISO27002, should also be implemented when a new software package is to be rolled out to meet a specific business requirement:

- Computer performance and capacity requirements should be assessed and taken into account in planning a roll-out.
- Revisions to, or establishment of new, error recovery and restart programs may be required.
- Routine operating procedures will have to be (re)drafted and tested to ensure that they are adequate.
- Appropriate new security controls will have to be put in place, consequent upon a risk assessment, for the new software system, of all aspects of the security arrangements upon which it has an impact.
- New user manuals and documented operating instructions may be required.
- New business continuity requirements may have to be dealt with.
- The impact on other software systems and processes should be considered and evidence sought that it will not adversely affect the running of existing systems, particularly at peak or critical periods such as month-end.
- Consideration should be given, in the risk assessment, to the possible effect that the new system may have on the overall security of the organization.
- Users should be trained in the use of the new system and the impact it will have on their current working practices.

It is often argued that it is safe for new, large-scale COTS systems to go live without any period of 'parallel running'. The risks of allowing them to do so should be very carefully assessed, back-up and contingency plans carefully thought out and tested, and appropriate insurance arrangements made. Where the organization has any uncertainty over the likelihood of the new system running 'out of the box', it should insist on stress-testing it by running it in parallel with the existing system in a safe test environment (that duplicates the operational one) until each of any key pre-identified stress points has been successfully overcome. Organizations should form their own views on these issues, not simply take the advice of external suppliers. This is particularly important for accounting and ERP systems, failure in the implementation of which can have devastating effects on the company concerned.

It is also important to have clear acceptance criteria (which clearly account for information risks) for any new communications systems and for anything that is connected to the internet. These systems should be demonstrably secure, and the system security risks analysed and appropriate steps taken, prior to connection.

Major system developments should be subject to a comprehensive project governance framework (for more information, see the IT Governance website), and in terms of testing and acceptance, this framework should at least include operational, stress and user acceptance testing. Depending on the risk assessment, the organization may even require an independent testing, verification and certification process, particularly to establish that the information security requirements have been met.

Protection of test data

Control 14.3.1 of ISO27002 says the organization should protect and control test data. As ISO27002 makes clear, this is a control that applies primarily to the development of operational programs. However, even the roll-out of commercial off-the-shelf (COTS) software packages should only be done after extensive testing that they are correctly configured, and this might involve using test data. If personal data are to be used, then their use will (in the United Kingdom) be subject to the Data Protection Act 2018. Such data should be depersonalized. If real operational data are to be used (and this is the most realistic form of testing) then there are potential vulnerabilities that ISO27002 recommends should be recognized in a risk assessment and protected by the introduction of appropriate controls. These should include:

- applying the same access control procedures as in the operational environment;
- a separate authorization process each time operational data is copied to a test environment;
- immediate erasure of operational data from the test environment on completion of testing;
- a process for ensuring that operational data are immediately deleted from the test system after use;
- and an audit trail of all related activity.

23

Supplier relationships

Supply Chain Risk Management (SCRM) is emerging as yet another component of effective enterprise risk management; all organizations depend, to one extent or another, on suppliers and, in today's interconnected world, organizations need to be able to rely on the confidentiality, integrity and availability of information shared with their suppliers, on the security of their supply chain connectivity and the reliability and robustness of their supply chains. Risks in supply chains range from external and environmental threats to geo-political ones and include issues like quality, security, service, resilience, integrity and health and safety. Control category A.15.1 contains a number of controls which work toward the overall objective of mitigating risks in relation to organizational assets that are accessible by suppliers; these controls should become part of any broader SCRM plan that the organization has in place. ISO/IEC 27036 (parts 1, 2 and 3) contain current best practice for supply chain risk management. ITIL organizations will integrate these controls into their supplier management processes.

Information security policy for supplier relationships

The starting point for the information security aspects of SCRM is for the organization to determine what its policy will be. Control 15.1.1 of ISO27002 focuses on the idea that how the organization had decided to mitigate its information security risks should be agreed in writing with suppliers and that an overriding policy should be in place to ensure that all supplier agreements are structured in line with a specific set of control requirements. Of course, any such requirements would have to be built into the existing procurement process (which means that buy-in from the procurement team will be necessary) and will have to have legal effect,

which means the corporate lawyers (along with those business units that consume any purchased products and services) will need to have input into the final form of key documents like the Standard Terms and Conditions.

Clause 15.1.1 of ISO27002 sets out a number of principles which, depending on the organization's risk assessment, could be part of its standard supplier contracting framework:

- Identifying the categories of suppliers that will be allowed to access the organization's information and information processing facilities. A practical starting point for this would be the list of suppliers identified during the scoping phase of the project, when documenting the requirements of internal and external parties and identifying outsourced services; as there are already existing arrangements in place with these organizations, it should be relatively easy to draw some general principles about what has previously been acceptable in terms of information access, to assess the risks and identify the balance of risk and benefit and, from there, arrive at an initial categorization of suppliers, the types of access that each supplier should have and how that access will be controlled and monitored. It should be borne in mind that one of the globally more significant data breaches of 2013 was effected by attackers taking control of an HVAC (heating and ventilation contractor) supplier's access to their retailer customer's building management systems to then access the retailer's in-house payment card systems.
- Creating a standardized supplier lifecycle management process which runs from research through selection to contracting, contract management and, finally, the purchase-to-pay process that covers individual transactions.
- How the principles as to which suppliers can have access to what are to be translated into actual supplier agreements and specific, actionable requirements, and what standard and what specific terms are applicable to which suppliers, and what form of documentation is required for what; this includes linking an assessment of supplier-related risk to the sensitivity of the information (in other words, there is a relationship between the classification system and the supplier risk assessment) the supplier needs in order to meet its contractual and business obligations.
- What monitoring and audit rights are built into supplier agreements and how these are linked to real-time monitoring of what suppliers do actually access and how they comply with the organization's information security policy and, where relevant, specific requirements – including the controls

for ensuring integrity and confidentiality of any information processed by the supplier – of the ISMS.

- What supplier obligation should be in terms of incident management, business continuity and resilience generally – which obviously includes the contingency arrangements that should be in place to deal at both the supplier and its customer in relation to disruptions, acts of nature, and the wide range of identifiable risks. Of course, there will be financial aspects to all these issues and putting in place really effective contingency measures shouldn't in any way undermine the importance of effective risk management through clear allocation of financial accountabilities.
- How personally identifiable information (PII) is handled; this is particularly important for organizations that collect personal information within the EU, as the EU GDPR forbids the movement of the data of EU residents to any country that does not have an EU-equivalent data protection regime. The USA, for instance, does not and so information systems that store personal data and are hosted with a US-based cloud services provider are quite likely to be a legal breach, unless the organization concerned has an EU–US Privacy Shield registration. The other key aspect to consider is that, under the EU GDPR, a data controller cannot transfer the accountability for the protection of personal data it has collected to any contracted supplier.
- Staff awareness training may be an issue that is identified in the risk assessment; this training might be applicable to both the supplier and the customer and could cover any aspect of the relationship where one or both parties need to understand the 'rules of engagement' and how specific, identified risks are to be managed and mitigated.
- How the transition (particularly for larger projects) from contract negotiation to delivery should be managed; this obviously covers maintaining information security through a transitionary process – covering, for instance, access to premises and facilities, to systems and to data.

Addressing security within supplier agreements

Control 15.1.2 of ISO27002 translates policy into action and requires the organization to ensure that all the security controls, service definitions and delivery levels identified in the third-party service contract are carried out.

This usually requires the dedication of adequate, appropriately skilled resources on either a full-time or a part-time basis. Substantial third-party contracts might require the creation of a management team and mechanisms for monitoring contract performance.

When an outsourcing contract is concluded, substantial information will need to transfer to the outsourcing supplier from the organization, and this transfer should be planned in detail and adequately resourced. A complete inventory of those information assets (hardware, software and information) that are to be transferred, together with their classification levels (which might necessitate an agreed mapping between both organization's classification schemes in order to ensure appropriate protection) should be agreed between the parties prior to finalization of the agreement, and this inventory should be used to ensure that all the assets actually are transferred.

Prior to transfer, there should be a risk assessment to identify the risks that there might be in the transfer process. These could range from access by unauthorized personnel through to accidental damage or loss. They should be listed in a project-level risk register (which is linked and subsidiary to the corporate-level risk register), and an appropriate control (within the organization's risk treatment framework) should be adopted for each of these risks.

Properly, the organization should carry out a risk assessment prior to entering into any significant third-party agreement and, after agreeing them with the contractor, incorporate into the contract those controls identified through the risk assessment. In addition, the contract should contain a clause that enables security enhancements to be required should there be a breach of any of the agreed controls during the contract period. The risk assessment has to take into account the fact that data will be stored at the contractor's premises and consider the possibility of their being compromised there. Sensible organizations will deploy standard procurement terms and conditions which cover all key legal and administrative issues, from IPR and copyright through to data protection and contractual liabilities. Issues that should receive particular consideration include:

- access to sensitive or critical information or applications that might be better dealt with in-house, the approval of asset owners for any outsourcing process, and the identification of key contact roles, screening for future hires, and how inadequate security performance might be dealt with, on both sides of the relationship;

- the security controls required, including access control, performance review, reporting, auditing, acceptable use, training and awareness and incident response and how compliance is to be measured;
- how activities and individual responsibilities are to be monitored;
- how security incidents are to be handled and supplier processes meld into the organizational continuity and resilience policy.

Again, there will be a judgement that the organization will have to make between the benefits it expects to gain through any supplier contract, whether provisioning or outsourcing, and the risks that the contract will bring. The controls that are adopted are, of course, designed to reduce this risk. It will also be important to ensure that the controls are not so tight that the contract is stifled from the outset, because that, in its own way, can be as big a risk as allowing too lax a regime to be implemented. This is an extremely difficult balance to strike, and the assistance of someone really experienced in negotiating long-lasting, secure supplier contracts might be sought early in the process.

In the outsourcing of IT, particular care will be necessary. A carefully thought-through control framework will be required. This should be specified in the outsourcing contract and should concentrate on staffing, access control and ensuring that, on an ongoing basis, an adequate level of assurance is obtained that systems, and system security, are being managed according to the contractually agreed standards. Thought should also be given to what other steps should be taken to ensure compliance with the contract. Comprehensive documentation of the relationship (including agendas and minutes of meetings, agreements on specific issues, etc) should be maintained in case of future dispute. Resilience arrangement should include what controls the organization has over any supplier sub-contracting and what fall back arrangements are pre-agreed to ensure smoothness of transition in case of a major disruption.

ICT supply chain

Control 15.1.3 of ISO27002 recognizes that most organizations that are in a company's ICT (Information and Communication Technology) supply chain do, themselves, have suppliers. Suppliers to your suppliers could introduce information security weaknesses which impact all their upstream

customers and customers' customers; if, for instance, a trusted supplier forwards an e-mail about a supply chain issue from one of their suppliers, there is a reasonable prospect the recipient will review it and click on any links to apparently urgent information. Weak information security down the supply chain can introduce threats that, because they are unexpected, can wreak significant havoc; attacking a target organization by exploiting security weaknesses and vulnerabilities further down its supply chain is therefore a logical avenue for an attacker.

ICT supply chain security is a strategic activity, relevant to larger organizations than to smaller ones. It is an additional activity to SCRM, which tends to focus on an organization's front and second rank suppliers; dealing with risk all the way down the ICT supply chain pre-supposes the organization has the available resources for addressing the issue, together with risks sufficiently significant to make this a relevant activity. At the heart of this specific control is the idea that the prime contracting organization drives a specific approach to supply chain security all the way down its supply chain. The steps for doing this are:

- work with Tier 1 suppliers to analyse their supply chains, and identify the generic risks that apply to particular types of supplier within the chain, or specific risks that might apply to specific suppliers, products or services;
- work with Tier 1 suppliers to agree information security standards and processes that are appropriate and necessary for the supply chain, focusing first on easily identifiable risks and then working to model particular threats and potential attack vectors in order to identify relevant controls;
- work with Tier 1 suppliers to determine how they will obtain assurance that required controls are in place. It's increasingly usual for supply chain assurance to be built on a framework of independent certification to standards such as ISO27001, ISO22301 and ISO20000;
- require Tier 1 suppliers to propagate the agreed security measures through their supply chains, through their own contract negotiation and management processes. Ensure that the contractual requirements will be extended to new suppliers and/or to suppliers of particular types of products or services – or components of them – where a significant risk has been identified.

In designing an ICT supply chain information security framework, there are two issues that have to be taken into account. The first is that Tier 1 suppliers

will incur a cost in developing their supply chains, and this will have to be factored into the commercial arrangements that any organization makes with its Tier 1 suppliers. The second issue is that there will be a number of suppliers in the supply chain – particularly suppliers of cloud and software services – where there is no room for contractual manoeuvre: their offer is on a 'take it or leave it' basis. In these instances, the sensible customer will identify compensating controls it can put in place to mitigate the effects of possible disruption in relation to their more intransigent suppliers.

Monitoring and review of supplier services

Control 15.2.1 of ISO27002 says organizations should monitor and review, on a regular basis, the performance of their suppliers. The key management step is to create a third-party contract management resource and a process (including standard reports, meetings, etc) that has a designated individual or (depending on the size and complexity of the contract) or department responsible for ensuring the contract requirements are met. While ISO27001 is particularly concerned with information security, the practical approach is for the contract management team to be responsible for all aspects of contract performance, including information security. This may mean that additional training is necessary, but the benefit in terms of clarity of process and accountability is clear. Key responsibilities should include:

- Monitoring service performance to ensure that the contracted levels are actually achieved, identifying shortfalls and agreeing how they should be rectified.
- Reviewing all records of security incidents (including audit trails), operational problems, failures, fault tracing and anything else likely to create a risk for the organization and ensuring that appropriate corrective action is taken. This may sometimes lead to escalation through the contractual escalation clauses, and the contract management team should have the skills and experience to manage such an escalation.

It is important that the third party designates an individual or, depending on importance, a team with whom the organization's contract management personnel can deal. The third-party unit needs to have sufficient authority to ensure the third party's adherence to the terms of the contract, and sufficient skill and experience to deal effectively with issues arising. The agreed contract management process should, for preference, be documented in the

outsourcing contract; this ensures that there is no room for vagueness about what is required, and in any case the organization may need to specify its right to monitor and audit the third party's change management processes, incident reporting and handling, vulnerability identification and correction processes, and to review the third party's own supply chain security.

Managing changes to supplier services

At the point that it transfers services to a third party, an organization loses the power to make direct changes to those services, whether to respond to changing business needs or to respond to new information security risks. Equally, once they are under the control of a third party, it is possible that changes that suit the third party might be inappropriate. It is important, therefore, that the outsourcing contract ensures that any changes are properly managed, and this is what control A.15.2.2 requires.

This control, which recognizes the central importance of risk assessments to effective management of information security, also recognizes that changes should be assessed in the light of how critical the affected business systems and processes actually are. The change management process should be an extension of that discussed earlier, with the exception that it will be an inter-organizational change process. It must therefore allow for approvals on both sides of the organizational barrier, and any barriers to the process must be identified and designed out as early as possible. Professional, experienced advice on change management within an outsourced function should be deployed early in the negotiation process.

The changes that the organization might require of its third-party contractor all have information security implications and therefore are likely to need a risk assessment followed by the identification and deployment of appropriate controls. Such changes include enhancements or changes to systems to handle changes to the current service offering; development of new applications or systems to meet new business needs; and changes that reflect changes in the organization's own internal policies and procedures, including those around information security and information security incidents. The third party may want to make changes to the services it provides to take account of network enhancements, new technologies (particularly those that reduce cost or improve efficiency), new products or new releases of existing products, new development tools, changes in its product or

service suppliers (eg a telecommunications supplier), and changes to (or in) physical locations. Again, all these should be identified in the outsourcing contract, and provision should be made for how possible changes that have not been identified should be addressed, to ensure that the organization does not come to a standstill.

24

Monitoring and information security incident management

The linkage between these two control categories – A.12.4, Logging and monitoring and A.16.1, Information security incident management – is an important one and, for that reason, we consider them together. There is also an important link between incident management and business continuity, and we will look at that in a subsequent chapter.

Logging and monitoring

Control 12.4 of ISO27002 has as its objective the recording of events, the collection of evidence and, of course, the detection of unauthorized activities. Monitoring will detect deviations from the controls adopted, including the access control policy, preventing repetitive abuse; monitorable events should be recorded to provide future evidence in dealing with security events. Such an approach allows the organization to review the effectiveness of its controls.

Event logging

Control 12.4.1 of ISO27002 requires the organization to produce, and keep for an agreed period, audit logs, which record exceptions and other security-related events to assist in future investigations and access control monitoring. Audit trails are essential when investigating what has gone wrong. They help establish events leading up to an incident as well as in determining indisputably the accountability for the event.

An event logging policy should therefore be determined by an appropriate management level, probably proposed by the information security adviser and agreed by the management information security forum. Extensive and detailed logs (which many systems, including Microsoft ones, can produce) may provide more (or less) information than is required, as it can be difficult to analyse a mass of data when looking for possible misuse. The policy should therefore reflect how logs should be configured to the risk assessment and logging needs of the organization and should reflect both best-practice guidance contained on the Microsoft security website (www.microsoft.com/en-gb/security (archived at https://perma.cc/YY9A-6W65)) and that available through CERT (www.sei.cmu.edu/about/divisions/cert/index.cfm (archived at https://perma.cc/C9ZJ-KUQ7)) and NIST (https://csrc.nist.gov (archived at https://perma.cc/Z5WL-42XB)).

As a minimum, event logs should contain user IDs; dates and times of log-on and log-off; terminal identity or location; details of attempted and successful and/or rejected access attempts to systems, data or applications; changes to system configurations; use of privileges, system utilities and applications; details of files and networks accessed and any alarms triggered; and details of either activation or deactivation of protection systems such as anti-malware software. Logs should be kept for a specified period in case they are needed for an investigation. While this period may depend on the volume of data, it is likely that a minimum period of one year would be appropriate. Access to the logs should obviously be protected, both logically and physically, from unauthorized access designed to cover up unauthorized activity. It is not self-evident that these logs should be kept by IT staff; it is more appropriate for them to be collected and retained by the organization's internal audit function. It should certainly not be possible for IT administrators to edit, erase or deactivate logs of their own activity, and the organization should take specific steps to ensure that administrator access rights and privileges are constructed so as to exclude this capability. Event logging will also encompass fault logging; this provides really useful data which should be analysed and corrective action to be taken. The most effective and practical way to handle this, for networks of any size (but there may need to be a cost–benefit analysis for the organization to ensure that this is appropriate), is to install some form of helpdesk software. (In an ITIL environment, this option is likely already to exist.) These packages log details of all user reports, and track action taken to deal with and close them out.

The ISMS should have clear procedures for how faults should be dealt with, setting out who is to take what action in respect of which faults and

the time period within which the issue is to be resolved. The same sort of detailed operating standards would appear in a third-party contract that specified the level of service that the third party was to provide.

Fault logs should be reviewed on a regular basis to ensure that faults have been satisfactorily resolved. The regularity will depend on the size of the network and the number of faults reported. In some organizations, it might be appropriate to review the log on a daily basis, while in others weekly might be enough. Independent checks should be made to ensure that the resolution is satisfactory for the user and that the recorded details are correct. This review should also ensure that any corrective action has not compromised other controls and that any steps were fully authorized.

Monitoring system use

Implementing 12.4.1 does, in effect, mean that the organization is putting in place procedures for monitoring user activity in relation to information processing facilities. While this is necessary to ensure that users are performing only authorized activities and is part of the 'prevention is better than cure' approach to information security, this monitoring should be carried out in line with relevant legislation (in the United Kingdom, the Regulation of Investigatory Powers and Human Rights Acts) which means this should be written into the staff internet acceptable use policy. A risk assessment should be used to determine the appropriate level of monitoring for individual facilities, and event logging should be automated. As already indicated, the items that should be monitored include details of authorized access, including details such as user IDs, dates and times of key events and their natures, the files accessed and the programs or utilities used. All privileged operations should be monitored, including the use of supervisor accounts, systems start-up and stop, and the attachment or detachment of input or output devices. All unauthorized access attempts should be logged, as should access policy violations and any notifications to network gateways or firewalls, and any alerts from intrusion detection systems. System alerts or failures such as console or workstation alerts or messages, system log exceptions and network management alarms should also be tracked. The audit functions in Windows should be used to carry out this monitoring and configured to reflect the risk assessment and in the light of advice on configuration both from independent experts and in documentation drawn from organizations such as CERT (www.sei.cmu.edu/about/divisions/cert/index.cfm (archived at https://perma.cc/C9ZJ-KUQ7)).

The result of the monitoring should be reviewed regularly, and the frequency of the monitoring should depend on the risks identified. The factors that will affect it include the criticality of the applications, the classification of the information involved, past experience of system abuse and the extent of system interconnection (particularly to the internet).

Protection of log information

At control 12.4.2, ISO27002 requires all the carefully collected log information to be protected against unauthorized tampering and access of any sort. It will be critical in any court case that the organization should be able to prove that its log information is reliable, and this can only be achieved if it is appropriately protected from the outset. Similarly, if log information can be altered or deleted, the organization may not get the warning of malicious activity that it relies on to trigger security steps. Protection involves ensuring that the log files cannot be edited or deleted, that any alterations to message types are recorded and that log file storage capacity is never exceeded, as this might trigger either overwriting of past events or a failure to record new events.

One of the biggest issues with audit logs is that they contain a massive amount of information, most of which is completely innocent because it records all the employees doing what they are supposed to be doing. It may be necessary, therefore (depending on cost–benefit and risk assessments), to have a process for copying specific types of information to a second log, which because it would be smaller would be more easily searchable. Even in this case, the original log needs to be retained for as long as is specified in the organization's data retention policy and may require a technological solution such as a data vault.

Administrator and operator logs

Control 12.4.3 of ISO27002 requires the system administrator and operational staff to maintain a log of their activities. In most organizations, this requirement applies to those staff responsible for the network system resources. ISO27002 recommends that their logs, which are usually kept in the server room and are in paper format (preferably not loose-leaf, as this makes it easy for pages to 'get lost'), should include:

- system or event start and finish times and who was involved;
- event information (files handled, processes involved);

- system errors (what, date, time) and corrective action taken;
- back-up timing, details of exchange of back-up tapes, handling of any other critical media;
- the name of the person making the log entry.

These records should be checked by the organization's internal audit function against the ISMS to ensure that procedures are being properly followed. Such checks can identify errors that one might not consider possible, such as the insurance company that backed up its main client-data holding server on to a head-cleaning cassette for in excess of three weeks. The problem was quickly rectified once identified, but if it hadn't been, it could under certain circumstances have had massive consequences.

An intrusion detection system could be deployed (or an existing one configured) to monitor the system and network administration activities of system and network administrators. Obviously, it would need to be deployed and monitored by someone other than the administrators, and it certainly has a cost of ownership and operation that should be assessed as part of the risk assessment that decides whether or not this is a cost-effective control.

Clock synchronization

Control 12.4.4 of ISO27002 says the organization should synchronize the computer clocks of all computers on its network for accurate recording. This is important because it ensures the accuracy – across all the organization's systems – of event and audit logs, which may be needed for incident investigation. Microsoft systems can operate real-time clocks, and on all computers within the domain the time should be set to a standard laid down in the ISMS such as universal coordinated time (UCT) or a local standard time such as GMT. Microsoft Windows Time Service should be configured to handle this process and to reference, on a regular basis, an external time source. It is important to ensure that the other servers on the network are correctly configured. Radio receivers that can provide a computer with the atomic clock signal might be considered as a labour-saving approach, since these can maintain temporal accuracy to the second. A risk assessment might be necessary to ensure that these do not also provide unguarded routes into the network.

Of course, it is also important that the ISMS lay down a standard date/time format and that this is implemented rigorously across the network. Local variations, such as daylight saving or cross-timeline networks, should

also be taken into account. Mobile users should be trained on how to manually synchronize time clocks if they log onto the network irregularly. Internal audit should carry out spot checks on a regular basis to ensure that the synchronization is effective.

A failure at this level could hamper event investigation, invalidate disciplinary action and fatally undermine court actions.

Information security events and incidents

Section 16 of ISO27002 deals with information security incident management and makes an important distinction between an information security event and an information security incident. An event is not necessarily an incident, whereas an incident will always start off as an event. In other words, there are a number of events that, because they are either expected or unexpected, might not significantly compromise the integrity, availability or confidentiality of the organization's information. Events are reported; incidents are managed – which means that there has to be a decision, for each event, as to whether or not it is an incident. The control objective is to ensure that events that relate to or might compromise information security, or weaknesses associated with the information systems, are communicated in a way that ensures timely action. The key management perspective is that however good the ISMS, there will be information security events. They may be accidental or they may be deliberate; a deliberate breach may be malicious or simply for the entertainment of a hacker. What matters is that the organization has in place a tested and thorough method for responding to the inevitable. Only in this way can the organization ensure the availability and integrity of its data. ISO/IEC 27035 is the Code of Practice that deals specifically with incident management and with the creation of an information security incident response team (ISIRT).

Incident management – responsibilities and procedures

Control 16.1.1 says the organization should establish management responsibilities and appropriate procedures to ensure a 'quick, effective and orderly response' to information security incidents. This forms part of the overall requirement for clear delineation of responsibility and clearly thought-through procedures for dealing with events before they become critical.

The first step is for the information security adviser to decide whether or not the event is an incident, and therefore what the appropriate response to it might be. Events that are likely to be classified as incidents, and therefore subject to the incident response procedure, include:

- Malware infections (there does need to be a distinction between those carriers that are caught and neutralized at the gateway and those that are successful in infecting a machine).
- Excessive spam (although 'excessive' may be a subjective term).
- Information system failures.
- Denial or loss of service, whether through hacker attacks or through provider action or inaction (a user may not always be able to distinguish between the two, and although the symptoms have different causes, it is worth treating them together). Recovery will involve specific action by the information security and IT staff, and may require the use of back-ups, uninterruptible power supplies (UPSs), and back-up sites and systems.
- Business information errors resulting from errors in input data (incomplete or inaccurate).
- Breaches of confidentiality or integrity.
- Misuse of information systems.

The incident response procedure (which should be a seamless continuation of the information security event reporting procedure and which should dove-tail into the non-conformity reporting and review procedures) should set out how to deal with each of these types of incidents and should include contingency plans that help the organization continue functioning while the incident is being dealt with. It should reflect the organization's risk treatment plan, and the criteria by which incidents are dealt with should be formally approved by the management information security forum. The board may need to sign off on those response criteria that involved a significant period or breadth of outage, or to which there may be significant costs. Contingency plans should, to the greatest extent possible, be tested prior to their being needed. Users should be trained in their use and involved in a regular contingency plan testing programme. Findings from this testing programme should be incorporated into the next version of each procedure, and all the documentation that describes the planned tests and their outcomes should form part of the ISMS records. The incident management (contingency planning) process should, therefore, encompass:

- immediately limiting or restricting any further impact of the incident;
- identification of the incident, and of its seriousness, with any analysis necessary to ascertain its cause(s), including the vulnerabilities it exploited;
- tactics (which are in line with organizational priorities and affordable) for containing the incident, so that damage does not spread;
- corrective action, which should be carried out only after appropriate planning (remember the PDCA model) and which should also aim to prevent recurrence;
- communication, certainly with those affected and with those involved in the corrective action;
- reporting the incident internally, almost certainly to the management information security forum (or whatever alternative oversight mechanism the organization has put in place).

The incident identification and corrective action stages of the process should include collection of any evidence that might later be necessary for analysing how the problem occurred, for deployment as forensic evidence in court (criminal or civil) that might follow or in relation to any regulatory breach that might have occurred, and for support in any compensation negotiations with software or service suppliers. The information security adviser needs to be aware of how to gather and secure evidence that might have a forensic value, and if he or she is not, arrangements should be made for a suitably qualified professional to attend an incident management planning and recovery meeting (but see below).

Overall, action to recover from security incidents and to correct system failures should be under formal control:

- Only identified and authorized personnel should have access to affected live systems during the incident management period.
- All emergency actions should be documented in as much detail as is possible at the time – which may require someone to be deputed to work alongside the information security adviser with the sole responsibility of recording decisions and actions as they happen (or, if it can be done only after the event, as soon as possible, while memories are still fresh).
- The escalation procedure needs to be clear, and management should be informed about events in line with a previously agreed set of criteria, so that the most serious events are notified to the board, less serious ones to the management information security forum only, etc. Line managers and

appropriate functional managers should receive the reports that the ISMS requires them to receive.

- The overriding objective must be to get business systems back into working order as quickly as possible and to confirm that their integrity has been re-established and that all the necessary controls are working again. As soon as possible after an incident, the information security adviser needs to be in a position to confirm that the integrity of the systems has been restored. This confirmation should be timed, dated and signed, and filed with the incident records in the ISMS documentation.
- Provision must be made for working beyond organizational and national boundaries, as some events and security incidents may transcend single organizations or countries.
- The communication plan needs to be clearly articulated, with roles and approved requirements understood.

Reporting information security events

Control 16.1.2 of ISO27002 says the organization should establish a procedure that ensures that information security events are reported to management as quickly as possible. Where the organization has an existing service desk and a process for reporting a fault, event or problem, it may well be sensible to integrate information security event reporting so that end users have a single, clearly identified method of reporting anything unfamiliar.

The event and incident reporting procedure should be integrated with the incident response and escalation procedure so that an effective overall process is established. Where this is also being integrated with an existing service desk, there will be need to be stage of 'triage' where the helpdesk operatives determine whether the event is an information security incident and to be dealt with differently than other events. ISO27035 describes a point of contact (PoC), which is the entity that is responsible for receiving, logging, and escalating as appropriate, information security events, and so on.

The event reporting procedure should start by referring to every employee's (and third party's) responsibility in respect of information security within the organization, as identified in their contracts of employment or other service contract. The organization should, from the outset, develop a

'no blame' reporting culture. This will encourage staff to report security events no matter the cause or who might be at fault. This is important, because the organization should want to ensure that appropriate staff are aware of events that might point to vulnerabilities that are widespread or critical and that need to be formally addressed. The vulnerability might be a result of weaknesses in training, or management, or system design, or anything – but if they are kept hidden, they cannot be tackled.

Security events fall, broadly, into four categories: 1) security breach (eg non-compliance with policies or guidelines, uncontrolled system changes, access violations, breaches of physical security arrangements); 2) threat (eg a member of staff identified as a hacker); 3) weakness (eg inadequate firewall control or spam filtering); or 4) malfunction (eg loss of service, equipment or facilities, system malfunctions or overloads, human errors, malfunctions of software or hardware). An organization might provide a covert duress alarm in high-risk environments (eg bank counters), the use of which indicates that the staff member is operating under duress. The associated procedure should set out clearly what the required response to such an alarm call is, and should ensure that anyone working in the exposed, 'high-risk' environment has appropriate training.

As information security is a fast-changing environment in which new threats emerge daily, it would be dangerous for a reporting procedure to be limited to specifically defined events. Every employee or contractor should be trained to be on the lookout for suspicious events that, in their opinion, might affect information security, and to report them as soon as possible. The reporting procedure can provide non-exclusive examples of events that might fall into each category.

In general, the reporting procedure should be quick and have redundancy built in. It should also allow for perceived emergency issues to receive more immediate attention. There should be some form of escalation procedure. While ISO27002 recommends that there should be a single point of contact for reporting all security events, we believe that this is often inadequate. All incidents could be reported to at least two people, who should both be required to take appropriate action.

The procedure might therefore require all incidents to be reported to the immediate line manager (or, for third-party contractors, the contractually identified organizational contact) or, in his or her absence, his or her deputy. It should simultaneously be reported directly to the information security adviser, who should have a widely advertised mobile telephone number reserved specifically for receiving these reports. Both these people should be

required to take immediate, appropriate action (within the limits of their training and proven competence) to deal with the issue and to communicate with one another as soon as possible thereafter to coordinate their actions. This structure would allow a line manager to pull someone off a particular task while the information security adviser arranges to isolate an apparently infected workstation or take more significant action in the event of a larger-scale attack.

Reporting should be by e-mail (unless for a suspected malware incident) and either by telephone or in person. The benefit of e-mail is that it provides evidence, later, of precisely when the event was reported and, from the employee's point of view, it proves that the report was made immediately. If, however, the employee's workstation is malfunctioning, reporting this fact electronically may not necessarily be wise! The organization's information security adviser has to decide how this circumstance is to be dealt with and incorporate, in the light of his or her risk assessment, appropriate instructions into the reporting procedure.

The time within which a response to an event is required should be clearly stated in the policy, in respect of each type of event. The procedure should require that the person who notified the event be told of the outcome within this period or, if there is to be a later investigation, within a specified period after its completion. There should be an escalation procedure so that the employee knows who else to report the event to if there is not an appropriate response within the defined period. Every organization will want to tackle escalation differently and in line with other escalation procedures and its existing culture. This is appropriate; the faster that the ISMS can be integrated into existing behaviours, the sooner it will be effective.

The event reporting procedure should also set out what steps are to be taken in response to the event and the time-frames within which they should be taken. The information security adviser should be asked to draft the event response procedure, creating an event report document that will be used to describe the event (and which contains a checklist that ensures all the critical information – date, time, what happened, screen messages, who did what, key strokes, etc – about the event is collected), as well as who reported it and when, and that sets out the action required to deal with it and the time-frame within which it needs to be taken. It should be clear to all employees (and third parties) that they are not to take any action on their own to deal with the event, and the procedure should remind everyone of the disciplinary process that will apply in the event of breaches of the ISMS.

The procedure should differentiate between standard responses (such as invoking a standard control specified in the ISMS in response to a related breach) and flexible, or discretionary, responses (dealing with an event, or a variation on an event, that has not previously occurred). It is important that this distinction is made, and that the procedure does not try to set out standardized responses to weaknesses or threats that it has not experienced before. The danger of such an approach is that the response will be inadequate or inappropriate. It is better to employ an information security adviser who has the skills and competence to evolve a new and appropriate response to a new threat; this characteristic is discussed in Chapter 4.

Certainly, the procedure should require that for serious incidents the information security adviser reports them to his or her superiors within a specified time period. On major issues (ones that, for instance, require the business continuity plan to be invoked or the computer infrastructure to be shut down), senior managers and, almost certainly, the CEO of the organization should be consulted.

Of course, as the organization accumulates experience of security events and improves its procedures as a result of controlling its response to them, so a bank of material that the organization can use in future training is built up.

Reporting software malfunctions

Control 16.1.2 of ISO27002 includes a requirement to report software malfunctions. Apparent software malfunctions are concerns for two reasons. The first is that they affect the ability of one (and potentially more than one) user to use the organization's information processing facilities. The second is that the apparent software malfunction might be some form of infection including spyware) that could destroy data, and thereafter the integrity of information, on the user's workstation and that could also, if not properly controlled, spread to other workstations on the organizational network.

The event reporting procedure should therefore incorporate the following steps:

1 Users should, for a start, have been trained to realize that any unexpected or unusual behaviour on the workstation is possibly a software malfunction.

2 Users should be required to note the symptoms and, if possible, any messages appearing on the screen.

3 Users should, if possible, immediately disconnect the workstation from the network and stop using it. The contacts identified in the event reporting procedure should immediately be notified.

4 The information security adviser should supervise the recovery of the workstation, and the work should be done by adequately trained and experienced staff. The workstation should not be re-powered while connected to the organizational network, and any diskettes in it should not be transferred to other computers until the incident has been completed and the diskettes cleared of carrying some form of malware.

Clearly, this type of incident cannot be reported using e-mail, as the procedure requires the workstation to be disconnected as quickly as possible from the network to avoid a possible problem spreading across the network.

An alternative reporting methodology needs to be available, such as by telephone. The person reporting the incident should be working with the same event reporting form as the person who experienced it; the objective is to ensure that as much as possible is gathered of the information essential to deal with the event.

Reporting security weaknesses

Control 16.1.3 of ISO27002 says users of the organization's information systems should note and report any observed or suspected security weaknesses in systems or services. Where weaknesses are reported directly to a service provider (which may be how the service contract is set up), they should also be reported internally. The service provider's response should be monitored and the effectiveness of its action to repair the weakness should be noted. This information has value in monitoring the overall contractual performance of the service provider; there is also the possibility that if a weakness is not dealt with quickly, the organization might be exposed, and therefore it is essential that progress in dealing with it is monitored.

The response to a reported weakness should, just as for security breaches, differentiate between those for which there is a standard response and those for which a non-standard but appropriate response will have to be determined. Most weaknesses will require a specific step, or series of steps, to be taken to deal with them. For non-standard weaknesses, the event reporting form should be signed off and dated by the security adviser once the required steps have been taken and the tests that demonstrate their effectiveness completed. For standard events, a sample can be signed off once the

information security adviser is confident, on the basis of systematic sampling, that the events are being appropriately dealt with. Over time, and on the basis of satisfactory sampling, the level and frequency of sampling can be decreased. The forms should, clearly, all be numbered and retained as part of the ISMS records.

Weaknesses should be reported through the same event reporting procedure as the one that deals with events. In other words, the organization should have just one, comprehensive event reporting system that deals with the entire range of possible security events. It is easier for staff to learn to use a single consolidated system than to give them a number of distinctions to make as to the type of event and therefore which system to use before they can make a report. This system should be referenced in employee and third-party contracts.

The event reporting procedure should clearly state that those uncovering a potential weakness should not, themselves, attempt to prove it. Not only might their own skills be inadequate to do this in a controlled manner, but such an action could (and should) also be treated by the organization as a potential misuse of the system and therefore likely to lead to disciplinary action.

Assessment of and decision on information security events

Control 16.1.4 expects the organization to have a structured and formalized approach to assessing information security events and incidents and deciding how to respond to them. In a smaller organization, the help/service desk may refer security events and incidents to the information security manager, who will determine their significance and decide on an appropriate response; in a larger organization, they might be referred to the information security incident response team (ISIRT) who will assess the incident – usually by reference to an agreed incident severity classification scale – and will initiate (usually) pre-planned and tested action to deal with the incident.

Response to information security incidents

Control 16.1.5 follows logically from the idea of a formal, structured process for assessing information security incidents. The information security manager, or the nominated individual within the ISIRT, should have

direct control over the response to the incident, utilizing wherever possible pre-agreed response routines. The standard response process should include the following:

- collecting evidence as soon as possible; evidence-based responses are preferable to emotionally-charged ones. Forensics analysis may be necessary (and having to hand a forensics kit and the contact details of known computer forensics consultants are a sensible part of the ISIRT armoury;
- identified escalation paths, both in terms of invoking the input of more senior management as well as in terms of invoking aspects of the organization's business continuity plan, are important. Something which starts with a minor denial of service (DoS) attack, which could be dealt with through an existing, pre-planned response, could escalate into a major, distributed DoS attack which is intended to create significant disruption and this would require a more strategic business continuity response. The concept of business resilience recognizes that organizations need to link management of information security and business continuity activities so that organizations are able to respond to the full range of possible disruptions.

Learning from incidents

Learning from incidents contributes to the continual improvement process. Control 16.1.6 says the organization should list, quantify and monitor the types, volumes and costs of incidents and malfunctions. This can easily be done by including in the incident response form sections that enable the base information to be gathered at the point of occurrence. It is sensible to use a standardized description for the majority of weaknesses and incidents, but it will not be practically possible to design a standard list until the organization has 12 months or more of practical experience of what sort of incidents occur frequently enough in its own environment for a standard set of terms to be adopted. At the outset, it will be enough to analyse incidents between the categories identified in the standard: incidents, weaknesses and malfunctions.

The information from the incident response forms should be collated on a regular basis, and every six months, or at least annually, the information security forum should review the information. The information security management forum should want to see an analysis (monthly, quarterly or

annually, depending on a risk assessment) of security incidents so that any trends can be identified, and resources reallocated to minimize appropriately the impact of any future threats. This review should also identify recurring or high-impact incidents, any sequence of low-level incidents, or any trends in events or incidents which, when considered together, might be the symptoms of a much larger or more significant single problem, any of which may point to the need for enhanced measures to limit the frequency, damage or cost of future occurrences. The half-yearly report should also be one of the documents taken into account whenever the security policy and the ISMS themselves are reviewed. Minutes of the forum meeting should set out what decisions, if any, were made in respect of the incidents review.

The United Kingdom's Centre for the Protection of National Infrastructure has, as part of its information sharing strategy to help combat the risk of electronic attack on the United Kingdom's information systems, developed a 'Warning, Advice and Reporting Point' (WARP) toolbox for use (free) by not-for-profit services and, with written permission, by commercial organizations. A WARP should improve information security by stimulating better communication of alerts and warnings, and encouraging incident reporting. The website to visit for more information is www.ncsc.gov.uk/information/what-warp (archived at https://perma.cc/337Z-MAA3), and development of a WARP would reflect continuous improvement in the ISMS.

Collection of evidence

Control 16.1.7 of ISO27002 says the organization should ensure that any evidence that it presents in an action (whether civil or criminal) against an individual or an organization conforms to the rules for evidence laid down either in the relevant law or in the rules of the court in the jurisdiction in which the action will be held. This requirement includes compliance with any published standard or code of practice for the production of admissible evidence, such that there is a reasonable prospect that the evidence produced will be both admissible and of an adequate quality.

This requirement is fairly obvious; the organization's lawyers are likely to provide this input at the point that a case is being prepared. At one level, therefore, no further action is needed at this point. At another level, of course, initially sensible systems will make this process that much easier. Such sensible systems will be based on retaining copies of all documents, ensuring that changes take place within a proper change management

environment and ensuring that policies and procedures are understood and observed.

It is also important to ensure that the procedure for dealing with security events and incidents includes a section on the gathering and preparation of evidence and that all personnel likely to have roles in investigating such incidents are trained in this aspect. It is not always clear, at the commencement of the investigation of a security incident, whether or not legal action may follow. It is possible, therefore, that without proper procedures, vital evidence may initially be lost, or later deemed inadmissable in court.

As ISO27002 sets out (in clause 16.1.7), the steps that should be included in the investigation procedure are the collection of originals of all relevant documents, including details as to who found it, where and when, with witness details if available. These records should then be securely retained so that they can be accessed only by authorized persons and so that there is no tampering with them. Copies of computer media (information on hard disks and on removable media such as CD-Roms and USB sticks) should also be retained, together with copies of access logs and details of any witnesses. Where copies are made of any computer media, this should be by a competent person, there should be a detailed log of the actions taken (what, how, time, etc), and these actions should be witnessed; one copy of this log and the computer media should be securely stored.

It may even be worth creating an event investigation kit, which would include a digital camera (set so that date and time are printed on the image), resealable and tamper-proof bags, digital recorders, etc. Such a kit should be secured when not in use, so that it cannot itself be tampered with.

Legal admissibility

It is essential that appropriate steps are taken, from the outset, to ensure that electronic documents will be admissible as evidence in court. Electronic documents (which include all e-mails) are always critical to any court case, and organizations need to take appropriate action to ensure that they can comply with court requirements for the production of evidence. The UK's ACPO Good Practice Guide for Digital Evidence is also internationally well regarded.

25

Business and information security continuity management

Control category 17 deals with information security continuity – with ensuring that the organization's information security objectives are achieved during any major disruption and are embedded in the continuity plans. Although the standard does not itself contain an explicit requirement for business continuity, and there are not explicit business continuity clauses in Annex A, the implementation of this control category depends on there being some form of business continuity plan. Any organization that is serious about ensuring information availability will have to put in place a business continuity plan to help it survive major disasters, counteract major disruptions to its activities and protect critical business processes from the effects of major failures or disasters and ensure their timely resumption. Far too many businesses fail because they did not have in place properly thought-through and adequately tested disaster recovery procedures. Unofficial statistics suggest that 80 per cent of organizations that suffer a disaster simply do not recover from it, but rather struggle through and then go out of business within a year or two.

ISO22301

Our view is that every organization needs a business continuity plan (BCP), which means addressing the whole issue simultaneously. Business continuity can be addressed by contracting with one of the many specialist business continuity vendors to help develop such a process (in which case, you will need to ensure that the information security aspects – which we will discuss separately in this chapter – have been adequately addressed and that specific

information protection and recovery components are built into and integrated with all other components of the plan), or it can be developed in-house, possibly using an external specialist vendor for testing the plan and for a specialized review of it.

A logical starting point for anyone developing a BCP is ISO22301 (www.itgovernance.co.uk/iso22301-business-continuity-standard). This is the international business continuity standard, developed from and replacing BS25999. Certification against ISO22301 will neither improve nor lessen the likelihood of a successful ISO27001 certification, and will not guarantee that you meet the information security continuity control requirements of ISO27001 Annex A, although it may have a positive effect on customers, suppliers and stakeholders.

ISO/IEC 27031 is the Code of Practice for what is called ICT Readiness for Business Continuity, or IRBC. It is a useful additional resource for organizations that want more extensive guidance on ICT business continuity.

The business continuity management process

All organizations need a managed process for developing and maintaining business continuity throughout the organization, and this must also address the information security requirements of continuity. The information security adviser could take the lead in setting up this process, which should be agreed by the information security management forum. The BCP process should:

- Ensure that the risks faced by the organization, in terms of their likelihood and potential impact, are understood, and that critical business processes are identified by means of risk assessments and their protection prioritized.
- Identify all the assets involved in critical business processes (by means of an extension to the asset inventory).
- Understand the range of impacts that interruptions may have on the organization and recognize that small incidents (power failures, virus attacks) may be as significant in terms of data availability, integrity and confidentiality as larger, more dynamic events (fires, bombs, floods).
- Ensure that adequate financial, organizational, technical and environmental resources are available to address the identified requirements.
- Ensure the safety of staff and the protection of information systems and organizational assets.

- Consider the purchase of insurance that covers the risks identified and ensure that premiums are kept up to date.
- Formulate and agree with line managers, and everyone likely to be affected, a business continuity strategy that is consistent with the organization's documented objectives and strategy. This needs to be no more than a single page that states clearly the overall approach to continuity, the prioritization of processes and the extent of training and review.
- Formulate and document detailed BCPs that are consistent with the strategy.
- Ensure that plans are regularly tested, lessons learned and plans updated.
- Ensure that the management of business continuity is as embedded into the organization's processes and culture as is information security generally, and that specific responsibilities for business continuity, and its information security aspects, have been allocated at an adequately high level in the organization.

A number of the steps in this process are discussed in more detail later in the chapter. The point of this clause is that all these activities need to be integrated into a whole process, so that loopholes do not develop and the planning is coherent and complete.

Business continuity and risk assessment

Every organization needs a strategy and plans for business continuity so as to counteract major system failures and to ensure timely resumption. Best practice in preparing a BCP is to carry out a business impact assessment and risk assessment. The first step is to identify each major process on which the organization depends. This should be straightforward, as exactly this was done in the early days of the project, when deciding project scope and identifying the assets within that scope. Estimate impact of disruption for each process and, on the basis of the organization's established risk appetite, determine how much pain can be endured. For each process, there will be a maximum tolerable period of disruption (MTPD), which could be measured in minutes, hours or days, and a recovery time objective (RTO) that is usually somewhat earlier than the MTPD.

It is also necessary to identify the various events that might lead to disruptions. There are threats and there are both major and minor potential

interruptions, and all these should be considered. The major external ones include bombs, terrorist activity, riots, fire and flood. The immediate external environment should also be considered and the possible risks assessed. There are particular locations where some such risks are obvious – the danger, for instance, of a vehicle coming off the road on a sharp bend and going through the wall of the business premises right there – and others where they are not – such as the possibility of the staff member taking the day's takings to the bank being mugged. Every possible external, physical danger, event or occurrence should be listed in a brainstorming session. Then there are the possible system-related risks. Malware, hacker activity and power failures are all possible dangers.

Once an exhaustive list has been compiled, a risk assessment should be carried out for each of them and for each of the critical systems and processes (not just the IT ones) within the business, and should involve the owners of the processes. The risk assessments should be carried out using the process and documentation developed for the ISMS and should determine the probability and likely impact on the organization of each of these possible interruptions. Impacts should include periods of time potentially out of action, and costs to the business in terms of repairing the loss and in terms of lost business, as well as the other possible damage that such interruptions might cause. Specific consideration should be given to the information aspects and impacts of these interruptions.

Not the least of the risks is the potential of injury to or death of customers, suppliers or employees while they are involved (or not) in organizational activity. There are the potential impacts of unavailability of suppliers, partners or staff (eg a public transport strike or a ban on aircraft flights might have extremely disruptive effects on the organization). The risk assessment should 'identify, quantify and prioritize risks against criteria and organizational objectives'; this means, for instance, that the risk assessment should identify the time within which the system has to be back up and running if damage is to be limited. It is likely that for a number of systems there will be a range of options where, for instance, if the system is up after five minutes the damage will be 5 per cent of the total cost or loss, whereas if it is up only after 30 minutes (or three hours, or three days) the damage will be 30 per cent of the total.

This type of analysis (which may require expert external guidance) helps the initial prioritization to be reviewed and contributes to the development of the business continuity strategy. Once the strategy has been developed, it

should be signed off by the board, and then work to develop an implementation plan can commence.

Developing and implementing continuity plans

Once one has a strategy, the organization needs to develop plans for maintaining and/or restoring business operations – and ensuring availability of information systems at the required level – in a timely manner (that is, within a specified timescale, which is arrived at as a result of the impact analysis) following an interruption to, or failure of, a critical business process. Individual BCPs should be written for each of the identified processes and should be written in line with the prioritization and RTO that was arrived at following completion of the impact analysis. This, usefully, will give the organization early recovery plans based on its biggest risks and its business objectives, rather than on the interests and skills of an individual manager. All the staff and resources that might be necessary to make a particular emergency plan work should be considered. Plans should be drafted by process or asset owners, in accordance with the planning process, and then submitted to the information security adviser for review.

The business continuity planning process should ensure that:

- There is a clear description (signed off by the board) of the circumstances in which the procedure is to be carried out.
- There is a clear description (signed off by the board) of what constitutes the maximum acceptable level of loss of information or services, and this criterion should drive all activity.
- All responsibilities and detailed emergency procedures for all identified interruptions are themselves identified and agreed internally, with clarity about who has the authority to invoke the plan.
- Emergency procedures are implemented quickly enough to allow recovery and restoration of the service within the specified timescale. Note that these need to allow for any internal or external business dependencies and for external contracts that may be in place. The services or resources – staffing, other resources, external contracts, fall-back arrangements – necessary to return the business, or the information systems, to an acceptable level should all be identified, as should the methods for accessing them.

- Agreed procedures and processes are documented and those involved in implementing the procedures must be involved in their creation. These plans, which must address organizational vulnerabilities, will themselves be highly sensitive documents and therefore need appropriate protection. Copies of them need to be securely stored in a remote location beyond the damage perimeter of the site to which they refer. One effective method of doing this is to provide members of the emergency response team with suitably protected CD-Roms or USB sticks (and adequately powered laptops) that contain the plans.
- Staff are trained in the emergency (both recovery and parallel operational) procedures, as well as in the overall crisis management situation. This training should be in the workplace and should involve carrying out the various actions specified in the emergency procedures until they are adequately memorized.
- Plans are tested and updated.
- The owner of the process or system is responsible for updating and maintaining the recovery plan and for ensuring that the central copies, and those stored remotely, are up to date.

ISO27031

ISO/IEC 27031 is the Code of Practice that deals specifically with ICT service continuity management. It provides useful guidance on ensuring that IT service continuity is planned and managed effectively within the overall organizational business continuity planning framework.

Business continuity planning framework

A complex organization should maintain a single framework of BCPs to ensure that all plans are consistent and that they all address information security requirements adequately, and to identify priorities for testing, maintenance and reassessment. When there are changes to BCPs (as a result of personnel changes that lead to changes in the owners of plans, or people affected by them, or the environment, or systems, for instance) or to the assets that they cover (for instance, if a new server farm location is created for the company) or to the environment within which they operate, then these effects could have an impact on other BCPs. It is therefore necessary to

have a framework, particularly within a large organization, to ensure that all the impacts of any changes are carried through all the plans. This framework should be integrated with the organization's overall change management framework.

The basis of this framework can be as simple as a matrix (an extension of the asset inventory) that identifies links between assets, processes, owners and continuity risks, so that, for instance, it is easy to see at a glance all the assets or processes that would be affected by fire or flood, or to see all the processes owned by particular individuals and the impact on the overall plan of failures in individual plans or failures in the dependencies of individual plans. It should also enable the information security manager (or, in some organizations, the risk manager) to identify critical dependencies, where more than one plan is dependent on a single person or resource whose own failure, therefore, will have significant ramifications for the entire organization.

Each process owner should be responsible for drafting and agreeing with the information security adviser a BCP for his or her process. This should include an emergency plan, a fall-back plan and a resumption plan, together with criteria that identify when each is to be invoked and the individuals responsible for each. The owner should also be responsible for maintaining his or her plan. Contractors should be responsible for fall-back arrangements for contracted technical services, although the organization's process owner should be responsible for the emergency plans.

The framework, which could be owned by the information security adviser, should provide for coordination of plans across an organization, setting planning and continuity priorities, and should cover individual domain plans, testing and continuous maintenance. It should also include:

- An escalation procedure, which identifies how to assess the situation, who is to be involved in the decision that an incident is to be escalated and who is told what, when and the criteria that will trigger escalation. This might include creating an emergency response team (ERT). It should allow for the possibility that nominated individuals could be absent when a continuity incident occurs and therefore should identify alternatives. This procedure should ensure that the appropriate level of management is informed within specified timescales of continuity incidents. This clearly means that contact information for all the nominated managers must be available; some managers may also have to provide emergency contact details for holiday periods or other periods of absence. This

escalation process needs to clearly indicate when BCP arrangements are to be invoked. Note that it is important to develop an understanding and culture whereby a manager is not chastised for escalating an issue he or she has been trying to manage for some time but has failed to control. The fear of chastisement could result in an incident not being reported upwards when it should be, perhaps leading to a significant increase in the time taken to resolve the incident, and/or its total impact once it is escalated. Chastisement should be reserved for the manager who does not recognize and escalate an incident in a timely manner.

- An internal mobilization and briefing procedure to ensure that everyone within the organization who has a role to play in dealing with the incident is alerted and appropriately briefed within a specified timescale. This involves the creation of a 'calling tree', which identifies how managers should cascade information through the organization by talking to their direct reports, who are then responsible for talking to theirs. Key individuals at all levels of the calling tree should have access to the whole tree, so that the cascade briefing can still happen even if some key individuals are not available to play their roles. This calling tree should be documented, with contact details kept up to date by the HR department, and it should be accessible to staff (particularly any who have critical roles in a disaster) even when the network is out of action.
- An external mobilization and briefing procedure should include all third-party organizations that may have a role to play in dealing with the disaster, and should include relevant and appropriate press contacts. There should be an appropriately trained media team capable of handling all media enquiries in relation to this event. It may also be necessary to include contact details for key customers, partners and suppliers, all of whom may need reassurance or other information in the case of disaster. All the public authorities (eg ambulance services, fire services) that may need to be notified or involved in the case of serious interruption or injury or loss of life also need to be included in this calling tree.
- The business continuity adviser should ensure that all individual BCPs are presented in the same format. This makes it simpler and easier for people to follow them in an emergency and for people not familiar with specific plans to understand them quickly. This format should show clearly the conditions under which the plan will be activated, how the situation should be assessed, who else might need to be involved and what type of actions might be required. It should show clearly who is

responsible for activating the plan. The size of the potential risk and the impact of time should also be considered.

- There should be a full range of emergency procedures, including how to deal with attacks on systems, fire, flood or other physical impact on the premises of the organization. There should be emergency evacuation procedures as well as appropriate accident procedures. These should set out precisely what has to be done by whom and should be clearly linked into the calling trees described above.
- Fall-back procedures should also be planned in advance. For each of the critical systems identified in the business impact analysis, there should be a plan that enables the service to move to and operate from alternative premises within the specified timescale, and that ensures that affected business processes are returned to operation within this timescale. The level of investment in alternative facilities and fall-back services should be driven by the risk analysis and impact assessment; clearly, processes and services that are essential for the survival of the organization need to be made operational extremely quickly. This fall-back planning should also identify minimum staff levels required to operate the fall-back services, and set out how these staff are to get to the fall-back site. Fall-back sites should be subject to their own risk assessment and should provide a level of security appropriate to the classification of the information to be processed there.
- Each plan should detail any necessary temporary operational procedures that will apply until resumption is complete. These will range from the handling of incoming telephone calls or customer/staff enquiries through to alternative goods delivery sites.
- Each plan should contain resumption procedures setting out how the service is to be brought back to normal operation. (It might need to include the setting down of details of suppliers of particular equipment, how that equipment is to be configured and what its dependencies and dependants are.) 'Normal' needs to be clearly defined (number of transactions, level of configuration, etc), so that it is possible to establish when it has been achieved.
- There should be a process for the testing of plans and for ensuring that lessons learned from tests are built into new versions of the plans. There needs to be a schedule setting out when and how the plans are to be tested. This should range from frequent tests for critical components of

the plans that have an everyday importance – fire alarms, uninterruptible power supply (UPS) tests, etc – to much less frequent tests for those components of plans that the risk assessment says are much less likely to be required (eg fire sprinkler systems). Common components of a number of plans (eg emergency evacuation procedures) should also be tested regularly.

- Staff and key personnel at contractors should all receive training in the BCPs that will affect them. In particular, they should receive training in recognizing the circumstances in which the plan may need to be invoked and to be aware of what changes in circumstances might affect the smooth operation of the plan when it is invoked and then ensuring that the plan is revised to take these changed circumstances into account. The process by which this training is to take place should be documented and there might even be an internal website where those who have responsibilities under the BCPs are able to share experience and learning.
- The responsibilities of all individuals who may have to take specific action as identified in one of the BCPs need to be specifically documented and added to the person's job description. Alternatives should be identified to deal with holidays and other absences, including unplanned and involuntary ones. The staff exit process should include a step that reviews whether or not there is a continuity plan role and ensures that the plan and any related calling tree are appropriately updated. Similarly, the new starter process should allow for a continuity plan role to be identified at this stage, and for the plan and calling tree documents to be updated.
- The critical assets and their whereabouts (together with any information necessary to access them) need to be documented for each of the components of each plan. Any special operating skill or knowledge that may be required to operate any of these assets also needs to be identified, together with provision for its availability.

Testing, maintaining and reassessing business continuity plans

The organization should test BCPs regularly and to carry out regular reviews to ensure that they remain up to date and effective, and that they address the requirements for information security. Untested BCPs are only slightly more useful than having none at all. The reality is that when a disaster strikes, people do not have time to search out the last copy of their BCP, check to see

whether or not it is up to date, work out what they are supposed to do and then do it.

A useful BCP is one that clicks into action smoothly and effectively when it is needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times and if the plan is then regularly tested by simulating the circumstances within which it has to work and seeing what happens. It is relatively easy to check whether or not the UPS runs, just as it is easy to confirm that the alarm bell works. There should be regular scheduled tests of such basic infrastructure.

The complex situations are the ones that have more than one variable, and BCPs and the simulation of triggering circumstances therefore need to be as realistic as possible. For instance, simply switching off the power to the server room to check that the UPS enables planned close-down of the server systems is not an effective test of the ability of the systems to survive a power failure. A generalized power failure will affect lighting and air-conditioning systems as well as the power supply to the servers. One needs to be sure that the air-conditioning will start up again after a power failure, or else the servers will overheat; and if the power failure happened after hours on a Friday night, the impact on the business of the resulting system crash could be severe, and certainly expensive. A live simulation of such an event would reveal this risk, and would lead to revisions of the BCP such that the air-conditioning was set up to restart properly and that an electronic temperature gauge inside the server room was linked to an alert service that could deliver a human intervention before the overheating became extreme.

BCPs often fail on being tested, perhaps because of wrong assumptions about people, hardware, software, the order in which things happen, interdependencies, changes in equipment or personnel, or oversights. Testing is therefore an essential component of the planning process. It is also an essential part of the maintenance process, as the organization needs to be sure that changes to equipment and personnel have been taken into account in revised plans.

There needs to be a detailed testing schedule that sets out clearly which components of the BCP are to be tested when, and who has the responsibility for the testing. Common components of a number of plans, and basic emergency procedures and warning systems, should be tested much more regularly than those that are more complex and less likely to be needed. The risk assessment determines which plans fall into which categories.

BCP tests should be monitored; the expected results of the test should be documented at the time that the testing plan is drawn up, and the actual

results should be recorded and compared with the expected ones. Differences should be analysed and appropriate changes made either to the plan or to the expected results in future. Further testing may then be necessary to ensure that changes to the plan do now produce the expected results.

There is a variety of scenarios to use in testing BCPs:

- Table-top testing of various scenarios involves an imaginary 'walk-through' of a BCP in a specific set of circumstances, using imaginary events and predicting what is likely to happen on the ground.
- Simulations are one of the most important testing approaches, as simulations also serve to train the people concerned and help identify other issues that could be critical but that have not been identified through the walk-through test.
- Technical recovery testing is designed to ensure that systems can be recovered efficiently, and this should start with ensuring that the system, or individual elements of it, can be restored from back-up and should then move on to test the restoration of individual servers, and then groups of servers, and then the whole server room. Weaknesses in any of these areas could be significant, and the processes and staff skill sets are critical. The availability of back-up personnel and third-party services, particularly out of hours, should be tested at this time.
- The testing of recovery into an alternative site (depending on the recovery strategy of the organization) is important. A prepared alternative site is essential for most organizations, otherwise fire, flood or any other major natural disaster may force the organization out of existence. It is important to test the ability to resume service and operations from an alternative site, getting back-up processes working and dealing with all the staff issues that there might be in such an event.
- Supplier facilities and services should be tested to ensure that they will meet their contract commitment. It is particularly important to test those components of their contract that relate to emergency or out-of-hours support as well as to stress-test the services to find out the point at which they might fail.
- Complete rehearsals of dealing with major disasters should be carried out at least annually and perhaps twice a year. These are best handled by using an outside, specialist organization to stage and manage the rehearsal, which should test all the components of the plan and all parts of the organization. The learning points from such a rehearsal are likely

to be numerous, and therefore the post-test review should be comprehensive and should involve feedback from all the people involved in it.

- Post-event trauma counselling may be a sensible component for the disaster recovery plan. It should perhaps be available after major rehearsals as well.

Of course, the need to test BCP arrangements in any one area diminishes if you have been unfortunate enough to have to invoke and test that aspect of the BCP arrangements in response to a real incident. The key is to remember to learn from the experience and make suitable improvements thereafter.

Change management is an essential component of maintaining BCPs. The organization's change management procedures should be extended to accommodate the needs of the continuity framework. This extension should simply be a requirement that for all changes in hardware, software and business processes, a check should be made as to the changes necessary in the related BCP and these should be carried out. Where the changes are significant (eg a complete change of server technology) then it may also be necessary to alter the testing schedule to ensure as early as possible that the revised BCP operates as required.

The way in which personnel changes should be fed into the plan was discussed earlier in this chapter. Individual BCPs, as well as the organization's overall continuity strategy, should be formally reviewed at least once a year and the information security adviser should be able, at this review, to demonstrate that all changes (since the last review) in personnel, addresses, telephone numbers, locations, facilities, resources, legislation, contractors, suppliers, key customers, business processes and, of course, risk and overall business strategy have been taken into account and appropriate changes made.

The IT Governance website provides resources that can be used in the development and maintenance of BCPs, including information about ISO22301 and various tools and standards which can be used in creating ISO27001-compliant contingency plans and which can be adapted to the needs of the organization.

Information security continuity

The key ISO27002 control objective, at 17.1 is to embed information security continuity into the organization's business continuity management

system (BCMS), to be sure that, in any situation where the BCMS was invoked, information security would be a natural part of the process. For example, the BCMS might require that, in the event of a fire alarm, all the internal electronic doors automatically unlock and open themselves; the ISMS should require that access to sensitive information in what are still officially secure areas should continue to be restricted.

There are three specific controls that talk to this control objective: planning, implementing and verifying.

Control 17.1.1 says the organization should determine its information security continuity objectives for adverse and disruptive circumstances, and should ensure that these are included in its business continuity (BC) or disaster recovery (DR) plans. Where such plans exist, it makes sense to explicitly capture information security requirements as part of the Business Impact Analysis phase of BCM. If it doesn't have any such plans, this control indicates that the logical approach is to assume that information security objectives are unaltered by the occurrence of a disaster and to plan accordingly.

Control 17.1.2 says the organization should establish documented procedures for achieving its information security continuity objectives. For preference, these should be an integral part of the BCMS or DR documentation. These procedures should include:

- identification of roles and responsibilities, within an appropriate emergency management structure (which must be derived from and operate within the normal day-to-day management structure) for appropriate experienced individuals within the BCMS team that will have specific information security continuity responsibilities, together with necessary training, competences, tools and authorities (the ISIRT, discussed in the previous chapter, might be an appropriate body to take on these continuity responsibilities);
- detailed procedures and plans for managing information security through a disruptive event, including planned and tested responses to specific scenarios;
- identification of which information security controls might be compromised by specific disruptions, and what compensating controls might be implemented in order to deal with vulnerabilities or risks that could be created in adverse situations. Effective tactics for attackers could for instance include a bomb scare; if the organization has no pre-determined

plan for responding to bomb incidents, it could evacuate a secure office, making unsupervised access easy for intruders.

Control 17.1.3 says the organization should verify that its information security continuity plans are effective. The only practical way to do this is by testing them preferably, again, as part of testing the organization's BC or DR plans. The testing objectives should follow the same structure as for BCP testing: tabletop tests will enable the organization to establish whether or not the structure of the plan will deliver the objectives; scenario (or live) testing will enable the organization to establish whether or not the ISIRT can deploy the plans calmly in a changing emergency situation and whether or not the integration of information security continuity with BC and DR plans is effective and seamless.

Control 17.1.4 deals with redundancy in information systems and says that, wherever the organization's information systems architecture does include built-in redundancy (fail over) capability, the organization's risk assessment should consider what additional arrangements might be necessary to ensure availability of critical information systems. This is a control which, to be systematically deployed, depends on an effective information classification system which pays appropriate attention to business requirements for information availability, and on clarity (which comes from a thorough asset inventory which includes identification of relationships and dependencies between assets) about the cumulative impact on key business processes of the failure of critical infrastructure components. Hardware (eg alternative power or telecoms sources, UPS), software (fault tolerant programs) and information (eg error detection and correction, auxiliary storage, RAID arrays) redundancy are typical categories of redundancy.

26

Compliance

Control 18 is intended to ensure that the organization avoids breaches of any criminal or civil law, as well as any statutory, regulatory or contractual obligations, and any security requirements. It deals with legal requirements, security policy compliance and technical checking, and with system audit. It is the last clause of the standard and it has two objectives with eight supporting controls.

The outline of relevant legislation in this, the legal requirements section of this book, is not intended to be authoritative. Current legal advice must be taken from qualified specialist legal advisers if an organization wants or needs to rely on any matter discussed here. Equally, it should be noted that this section is dealing with current compliance issues for organizations based or operating in or supplying either the UK or US market. Laws are likely to be different in other countries, and therefore organizations seeking certification that are based elsewhere should take specialist local advice. Organizations based in a jurisdiction with operations elsewhere in the world will need to deal with the local legal requirements as well as those of the foreign countries in which they operate, and again specialist legal advice should be taken.

E-commerce (even if the organization is based in one jurisdiction) could potentially take place in a multitude of countries, and the law in this area is constantly changing and developing. Any organization that is trading across the web without limits on who may access its website should take specialist advice to ensure that contractual and trading terms are watertight and that issues of jurisdiction and which law (that of the country in which the server is based, or the organization is based, or the customer is based, or to which delivery is made) will apply to any transaction have been resolved, and to ensure that there is an appropriate acceptance and/or waiver of liability on the entrance to the website.

Identification of applicable legislation

Control 18.1.1 of ISO27002 says the organization should explicitly define and document the statutory, regulatory and contractual requirements for each of its information systems, and this documentation should be kept up to date to reflect any relevant changes in the legal environment. The specific controls and individual responsibilities to meet these requirements should be similarly documented and kept up to date. The ISMS should already contain a complete list of all the data assets and processes in the organization, together with ownership details (see Chapter 8).

A sensible way to tackle this requirement is to create a database of applicable legislation (which will need to be updated as and when laws change) that identifies relevant laws, the specific clauses which may be applicable, and which links those specific clauses to individual controls in the ISMS. For each regulatory or contractual requirement on the database, someone in the organization should have allocated responsibility for ensuring compliance.

Of course, in an integrated management system there would be an integrated approach to tracking legal and compliance developments in all the components of the system. Information security, health and safety, environment, quality, human resources, commercial and other issues would all be systematically tracked and appropriate steps taken towards compliance inside the organization.

The legislation that any organization might need to identify could include, but is not necessarily limited to:

- *EU regulation.* EU directives have been, and will continue to be, significant drivers of UK regulation. The two most important EU instruments, from the perspective of this clause of the standard, are the EU General Data Protection Regulation (GDPR) and the EU Privacy Directive of 2003. These instruments give the context for the UK legislation identified and discussed below, and for any changes that may occur in future.
- *UK legislation.* Intellectual property rights (IPR), through the Copyright, Designs and Patents Act 1988 (CDPA), are one of the most obvious legal issues for most information processing systems, but there is a web of other relevant legislation. The Companies Act 2006, which consolidates and replaces all the previous UK Companies Acts, contains a number of important provisions regarding electronic records, electronic trading and electronic communications. The next most important of these laws is the Data Protection Act 2018 (DPA), and in addition to this there are the

Human Rights Act 1998 (HRA), the Regulation of Investigatory Powers Act 2000 (RIPA), the Computer Misuse Act 1990 (as updated by the Police and Justice Act 2006), the Electronic Communications Act 2000 and the Privacy and Electronic Communications Regulations 2003 (as amended). The Freedom of Information Act (FOIA) was passed in 2000 and, while primarily applicable to public bodies, it has the potential to force into the public arena confidential commercial information about (for instance) public-sector contracts.

- In the United Kingdom, there is a complex array of anti-money laundering laws including the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003. Compliance with this legislation means that detailed client verification records need to be maintained and kept secure.
- More recent UK laws include the Bribery Act, an array of Crime and Security Acts, plus assorted legislation dealing with identity cards and electronic money.
- There is an increasing amount of corporate governance legislation in the United Kingdom, which will require the collection and storage of commercially sensitive data in order to satisfy reporting obligations. In order to comply, directors will also need to satisfy themselves that the IT system itself does not pose any operational risks to the company. These requirements, originally contained in general legislation such as the Companies (Audit, Investigations and Community Enterprise) Act 2004 were carried forward to the Companies Act 2006. There is also sector-specific regulation enforced by bodies such as the Financial Services Authority.
- US *legislation*. Relevant US legislation and regulation include the Gramm–Leach–Bliley Act (GLBA), dealing with consumer financial data; the Fair Credit Reporting Act (FCRA), designed to protect people from identify theft; the Health Insurance Portability and Accountability Act (HIPAA), which requires healthcare organizations (and their business associates) to protect – and keep up to date – their patients' healthcare records; the SEC's Regulation FD, which bars selective disclosure of material non-public information; the SEC's rule 17 a-4, which requires broker dealers to retain trading records (therefore including e-mails, etc) for six years; section 404 of Sarbanes–Oxley (the overall importance of which is much greater than this single issue), which requires companies to safeguard (among other assets) their information, including e-mails,

attachments, etc; the California Online Privacy Protection Act of 2004 (OPPA), which requires websites serving Californians (irrespective of their geographic or jurisdictional location) to comply with strict privacy guidelines; the CAN-SPAM Act, the Millennium Digital Copyright Act, FISMA and a growing number of state information security and data breach laws (such as the Californian Senate Bill 1386), which require notification of breaches of personal data security.

Most recently, California's Consumer Privacy Act brings some of the EU GDPR regulatory heft to the USA and has triggered a federal-level review of US privacy regulation. Of course, the huge growth in anti-money-laundering regulation, including the requirements of the international Joint Task Force and the US Patriot Act, broadens the requirement on organizations to verify client details, and therefore to keep those personal details secure and in line with applicable data security regulations.

UK legislation

In the United Kingdom, there are now over 70 laws that, to one extent or another, may need to be reflected in the ISMS. A current list is included in the Vigilant Software Compliance Manager. The most important legislation includes the following.

THE DATA PROTECTION ACT 2018

The UK's Data Protection Act 2018 (DPA), which puts the EU GDPR into UK statute, requires any organization that processes personal data to comply with six data protection principles. These are that personal data must be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date;
5. retained only for as long as necessary;
6. processed in an appropriate manner to maintain security.

The DPA 2018 is concerned with every conceivable category of personal data that relates to an identifiable natural individual and includes information such as ide ntification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental,

economic, cultural or social identity of that natural person. Under the terms of the DPA, 'processing' includes any operation performed on personal data, and the requirements apply to both electronic data and paper records (if they are contained in a 'relevant filing system'). The precise definitions of what is and what is not covered are set out in the GDPR.

Any organization that is going to collect personal data (a data controller) must register with the Information Commissioner. Notification lasts one year and must then be renewed.

The DPA covers all activities that involve processing personal data, including CCTV records, websites and internet activity, recruitment and selection of staff, employment records, staff monitoring (including, for example, checking telephone records or internet use) and information about workers' health.

The Information Commissioner's website provides detailed guidance and a number of codes of practice (some general codes and others specific to the public or private sectors) on the steps necessary for an organization to comply with the DPA. In that guidance, the Information Commissioner describes the approach that an organization should follow in its effort to comply with the sixth data protection principle. This approach is in line with ISO27001. It would be fair to assume from this that implementation of an accredited ISMS would be regarded as an appropriate step to comply with the requirements of the sixth principle of the DPA.

The key point is that data controllers and data processors – those organizations that process data on behalf of a data controller – must comply with the DPA; failure to do so could result in substantial fines for organizations, and particular attention should be paid to the requirement to keep data secure. The Information Commissioner has the power to levy fines of up to 4 per cent of global turnover for the most serious breaches of the DPA.

In particular, the GDPR requires organizations to take all appropriate steps to protect personal data from likely compromises to its confidentiality, integrity and availability and to do so after taking account of vulnerabilities, impacts and the 'state of the art'. The risk-driven approach of ISO 27001 supports the requirements of the DPA.

DPA 2018 requires organizations that suffer data breaches (where there is a risk to the rights and freedoms of data subjects) to report them to the Information Commissioner within 72 hours. It also confers on data subjects the right to bring complaints to supervisory authorities or to bring court actions in circumstances where they consider their rights as data subjects to have been transgressed.

THE PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS 2003 AND 2011

The Privacy and Electronic Communications Regulations 2003 came into force on 11 December 2003 and superseded the earlier Telecommunications (Data Protection and Privacy) Regulations 1999. The Information Commissioner is responsible for enforcing them, and there is a section on the Information Commissioner's website dealing with these regulations.

The regulations cover use, by telecommunication network and service providers and by individuals, of any publicly available electronic communications network for direct marketing purposes, and any unsolicited direct marketing activity by telephone, fax, electronic mail (which includes text, video and picture messaging, SMS and e-mail) and automated telephone calling systems. The key right conferred both on individuals and on corporate entities is the right to register their objection to receiving unsolicited direct marketing material, and it provides a mechanism for doing this. A number of requirements, including in some circumstances the obligation to obtain the prior consent of the person to whom marketing messages are to be directed, are imposed on direct marketers, and these will intersect with obligations under the DPA; organizations have to ensure that they comply with both. The 2011 amendment introduced a requirement to obtain the explicit prior consent of the surfer before installing a cookie in the browser. The Information Commissioner's website supplies, and keeps up to date, detailed guidance on these regulations. The detailed law around data protection and privacy is changing as cases work their way through the courts. Any organization engaged in direct electronic marketing of any sort needs to take appropriate legal advice and ensure that its operations remain in line with the law.

THE FREEDOM OF INFORMATION ACT 2000

The Information Commissioner enforces both the Freedom of Information Act 2000 (FOIA) and the Data Protection Act. The FOIA provides a general right of access to all types of information held by public authorities and those providing services for them. The FOIA is 'intended to promote a culture of openness and accountability amongst public sector bodies, and therefore facilitate better public understanding of how public bodies carry out their duties, why they make the decisions they do, and how they spend public money'. Only public authorities are covered by the Act and there is a long list, at Schedule 1 of the FOIA, of all the organizations covered. It basically includes any public body.

The FOIA came fully into force on 1 January 2005, and the first adoption of a publication scheme under the FOIA was by government departments and their agencies in 2002. The rights of individuals to access information held by these organizations, and the responsibilities of the organizations, can be explored further on https://ico.org.uk (archived at https://perma.cc/6BTV-VF5H).

Private companies should note that one of the clear consequences of the FOIA is that details of their previously confidential public-sector tenders and contracts could now be made public, irrespective of any previous confidentiality clauses. This is a key area on which private-sector companies may urgently need to take contract-specific professional advice; certainly, their commercial practices may need to be adjusted to reflect the risk of disclosure.

The Information Commissioner is also now responsible for the Environmental Information Regulations 2004 (which also came into force on 1 January 2005), which enable people to access environmental information held by or on behalf of public authorities and those bodies carrying out a public function. Technically, any environmental information request is an FOIA request, but, as environmental information was exempted in the FOIA, these regulations are necessary. As part of the requested information might also be personal information (eg if the applicant is a subject of the information request), these regulations intersect with the DPA.

Public authorities will take appropriate legal advice on the issues contained in the three pieces of legislation; it is expected that use and practice, court cases and ministerial interventions will all contribute to a changing privacy landscape. Introduction of a personal identity card will dramatically shake up the whole area.

THE COMPUTER MISUSE ACT 1990

The Computer Misuse Act 1990 (CMA) was designed to set up provisions for securing computer material against unauthorized access or modification. It created three offences: the first is knowingly to use a computer to obtain unauthorized access to any program or data held in the computer; the second is to use this unauthorized access to commit one or more offences; the third is to carry out an unauthorized modification of any computer material. The CMA allows for penalties in the form of both fines and imprisonment.

The CMA basically outlaws, within the United Kingdom, hacking and the introduction of computer viruses. It initially had a significant impact on

the computer policies of universities, often seen as the source of much of this sort of activity. It does have other implications for computer users in the United Kingdom. Anyone using someone else's user name without proper authorization is potentially committing an offence. Anyone copying data who is not specifically authorized is potentially committing an offence. It also has relevance for organizations whose employees may be using organizational facilities to hack other sites or otherwise commit offences identified under the Act. The organization should take full advantage of the RIPA (see below) to ensure that staff are complying with the law.

The United Kingdom's All Party Internet Group (APIG) reviewed this Act in mid-2004 and recognized that it had been ineffective, largely through inadequate enforcement resourcing. It recommended a limited number of changes to the CMA and a number of other actions by other bodies to improve the legal environment for computer security. This led to the Police and Justice Act (2006) which updated and modified the CMA.

THE POLICE AND JUSTICE ACT 2006

Clauses 35–38 of the Police and Justice Act 2006 (which also deals with many other issues) amended the CMA as follows:

- The maximum sentence for 'unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer' (aimed primarily at denial-of-service attacks, but with a far wider effect) was doubled from five to ten years.
- They created an offence of 'making, supplying or obtaining articles for use in an offence' as defined in the CMA, as amended. While it is claimed that this provision, which is clearly intended to deal with hacking tools, may have the unintended consequence of impacting ethical hacking and penetration testing, the wording of clause 3A indicates that there will only be an offence if the supply of hacking tools is done in the intention or belief that they will be used in (or used to assist) the commission of an offence as defined in the CMA (as amended).

THE COPYRIGHT, DESIGNS AND PATENTS ACT 1988

The internet starting point for organizations that want detailed advice on intellectual property is the Intellectual Property Office. The principal legislation on copyright can be found in the Copyright, Designs and Patents Act 1988 (CDPA). It has been amended a number of times and there is no

official consolidation of it. A list of the most important pieces of legislation that have amended the 1988 Act and some other information about the legislation can be obtained from the UK Intellectual Property Office (www.gov.uk/government/organisations/intellectual-property-office (archived at https://perma.cc/J6EG-3ZL2)). This is a complex and difficult area for any organization that deals in intellectual property, and appropriate professional advice should be taken from a firm that specializes in this area.

Organizations with valuable digital assets should also track the developments in steganography, which is a method of hiding information in other data, such as voice communications, visual images and music, in order to provide forensic evidence of copyright ownership and trace the source of infringing material. This might also be called 'digital watermarking' and is likely to become an important part of copyright management on the internet. There are a number of companies offering competing digital watermarking technologies, both to create and to view digital watermarks.

In the United Kingdom there are a number of collective bodies that handle licensing for specific sectors of the creative industries. They include the Copyright Licensing Agency (CLA), a non-profit-making company that licenses organizations for photocopying and scanning from magazines, books and journals. The CLA was established in 1982 by the Authors' Licensing and Collecting Society (ALCS) (www.alcs.co.uk (archived at https://perma.cc/GBZ6-SXRD)) and the Publishers Licensing Society (PLS) (www.pls.org.uk (archived at https://perma.cc/82V3-PFJ4)) to perform collective licensing on their behalf. It provides a fair and effective way of collecting fees due to authors and publishers for the reproduction of their work. CLA licences permit the photocopying, scanning and e-mailing of articles from trade and consumer magazines, journals, books, law reports and press cuttings without having to seek permission from the copyright owner each time. As a matter of course, any organization that is likely to need legal access to such publications should get an appropriate CLA licence.

THE ELECTRONIC COMMUNICATIONS ACT 2000

The Electronic Communications Act, along with the Electronic Signatures Regulations 2002 and the Electronic Commerce Regulations 2002, is designed to regulate the use, within the United Kingdom, of cryptography and to make provision for the use of electronic signatures. Essentially, there are fall-back powers (not yet exercised) to create a central, statutory but voluntary register of approved providers of cryptography services in the

United Kingdom, and there are a number of regulations affecting how these approvals are given. The Act also provides for appropriately authenticated electronic signatures to be used in electronic commerce and allows for them to be admitted as evidence in court.

THE HUMAN RIGHTS ACT 1998

The Human Rights Act 1998 (HRA) was enacted in October 2000. It incorporates into UK law the principles of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention). Most of the rights within the Convention are qualified, in so far as they are subject to limitations if the employer can show necessity to protect the rights and freedom of others. In particular, an employee could argue in a court or tribunal that monitoring or tapping of the employee's work telephone or e-mail or internet activity by the employer was a breach of the employee's rights under the Convention.

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Section 1 of the Regulation of Investigatory Powers Act 2000 (RIPA) makes it unlawful intentionally to intercept communications over a public or private telecommunications network without lawful authority. Section 3 allows a defence if it can be reasonably believed that both parties consented to the interception. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 were issued under the powers of the RIPA and these allow employers to monitor employee communications where the employee has not given express consent, provided that the monitoring is for one or more of the following purposes. It should be carried out to:

- record evidence of business transactions;
- ensure compliance with regulatory or self-regulatory guidelines;
- maintain the effective operation of the employer's systems;
- monitor standards of training and service;
- prevent or detect criminal activity;
- prevent the unauthorized use of computer or telephone systems (ensuring that the employer's policies are not breached).

Employers also have to take reasonable steps to inform employees that their communications might be intercepted. This means that employers must

introduce acceptable use policies (see Chapter 17) that set out for the employees the employer's right to monitor such communications.

CODE OF PRACTICE

The Information Commissioner published a code of practice called 'The use of personal data in employer/employee relationships'. This code is more restrictive than the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 issued under the power of the RIPA. The code argues that the interception of personal electronic communications will almost certainly be covered by data protection principles. It says that unless the circumstances justify the additional intrusion, an employer should limit monitoring to traffic data rather than the contents of the communication, undertake spot checks rather than continuous monitoring, as far as possible, automate the monitoring so as to reduce the extent to which extraneous information is made available to any person other than the parties to a communication, and target monitoring to areas of highest risk.

While there will probably be a series of court and tribunal cases over the next few years that deal with the conflicts between the HRA, the RIPA and the code of practice, employers certainly need to introduce an acceptable use policy if they wish to be able to take legal or disciplinary action in respect of inappropriate employee behaviour.

Network and Information Security Directive

The EU's Network and Information Security Directive requires member states to legislate for Critical National Infrastructure organizations to focus on the availability of crucial network and information systems. It became law in the UK on 10 May 2018. It affects operators of essential services (OES) and digital service providers (DSPs) that are established or which offer services within the EU. The regulations apply to large organizations and, apart from imposing cyber security obligations, the regulations also require an incident response process as well as incident notification. More detailed information is available on https://www.itgovernance.co.uk/nis-directive (archived at https://perma.cc/HU7R-ZG9F). ISO 27001 is an ideal standard for organizations implementing NIS; given that all such organizations are also subject to GDPR, ISO 27001 can be used to create an integrated and compliant information security and incident response management system that is both cost effective and compliant.

US legislation

There is not yet any federal data protection legislation similar to that found in the EU or in countries such as Canada, Australia and South Africa. Most individual states have enacted their own laws around information security (eg 201.CMR.17, the Massachusetts law protecting personal information). Most of the individual states within the United States now have a data breach law, which sets out requirements and penalties for organizations that experience a breach that compromises personal information. A list of state data breach laws is maintained at www.ncsl.org/default.aspx?tabid=13489 (archived at https://perma.cc/VME6-DU6H). Work in the United States is also ongoing around the development of a National Office of Cyberspace and around the cyber security aspects of homeland security.

HIPAA

HIPAA, a US federal law passed originally in 1996, applies to health plans, healthcare clearinghouses and healthcare providers, which are known in the Act as 'covered entities'. The Act requires healthcare organizations to protect – and keep up to date – their patients' healthcare records (which includes patient account handling, billing and medical records), in order to streamline health industry inefficiencies, reduce paperwork, make the detection and prosecution of fraud easier, and to enable workers to change jobs more easily, even if they have pre-existing medical conditions. The information security requirements of the Act are contained in Health Insurance Reform: Security Standards; Final Rule (45 CFR Parts 160, 162 and 164; 20 February 2003). This requires covered entities to 'ensure the confidentiality, integrity, and availability of all electronic protected health information they create, receive, maintain, or transmit' S 164.306(a)(1); to 'protect against any reasonably anticipated threats or hazards to security or integrity of such information' ibid (2), and to 'protect against any reasonably anticipated uses or disclosures of such information that are not permitted' ibid (3). The compliance date, for all covered entities with the exception of small health plans (which had an extra year) was 20 April 2005.

The Administrative Simplification (AS) Provisions state the specific rules that institutions must implement in order to comply with HIPAA; these include rules for EDI, for electronic signatures and standards of privacy. They are intended to be technology-independent and each institution is expected to deploy the technology it considers appropriate.

The HITECH Act of 2009 was intended to accelerate the federal initiative for adoption of electronic health records (EHR) and extended the requirements of HIPAA to business associates of covered entities.

GLBA

GLBA, passed in 1999, applies to financial institutions and their service providers. The Financial Information Privacy Protection Act (to give it its full title) covers all US-regulated financial services corporations, and charges their boards with protecting their customers' personal information against any 'reasonably foreseeable' threats to its security, confidentiality or integrity. GLBA also applies to a wide range of 'non-bank' managers and the Federal Trade Commission (FTC), which is responsible for enforcing the Act, requires compliance with both the letter and spirit of the Act. GLBA requires management to develop, draft, approve and implement an appropriate information security program as part of their normal accountabilities. The information security requirements of the Act are contained in the Standards for Safeguarding Customer Information: Final Rule (16 CFR Part 314, May 23, 2002 – the rules issued by the other banking agencies are substantively identical). The rules relate to 'nonpublic personal information' which consists of 'personally identifiable financial information' and includes any information collected through a 'cookie'. The purpose of GLBA is defined as setting standards for 'developing, implementing, and maintaining reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information' S 314.1(a).

The GLBA Final Rule is explicit in requiring financial institutions to 'identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information'; to consider risks in each area of operations, particularly 'information systems, including network and software design, as well as information processing, storage, transmission and disposal', S314.4(a)(2); and to be responsible for 'detecting, preventing and responding to attacks, intrusions, or other systems failures', S314.4(a)(3).

The interplay between regulatory regimes is exemplified in the statement that GLBA does not 'modify, limit or supersede operation of the FRCA', and does 'not pre-empt any state law that provides greater protections'.

THE FAIR CREDIT REPORTING ACT (FCRA)

The FCRA was passed in 1999. It is designed to 'promote accuracy and ensure the privacy of the information used in credit reports', applies specifically to consumer reporting agencies (such as credit bureaus) and is enforced by the FTC. It is underpinned by a range of state laws.

CAN-SPAM ACT

The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act) of 2003 set national standards for the sending of commercial e-mail and requires the Federal Trade Commission (FTC) to enforce its provisions. This act permits e-mail marketers to send unsolicited commercial e-mail as long as it contains: an opt-out mechanism, a functioning return e-mail address, a valid subject line indicating it is an advertisement and the legitimate physical address of the mailer. The bill includes many other provisions, such as the formation of a national do-not-spam list, and the prohibition of certain e-mail address collection methods. The idea of a do-not-spam list was not a good one.

Many states have also enacted anti-spam laws, some of which prohibit sending unsolicited commercial e-mail to state residents unless they have specifically opted in to receive it.

Enforcement of legislation has been, in most jurisdictions, both weak and inconsistent. This is partly because enforcement is technologically difficult and partly because so much spam originates in jurisdictions beyond the control of any individual state. However, where authorities and affected organizations determine to take action, they do get results, as actions by various ISPs, by Microsoft, the jailing of a number of spammers and the April 2005 bankruptcy of the internet's then third biggest spammer, all demonstrate.

The real anti-spam action, though, is being taken by individual organizations. The most effective defences against spam are at the ISP level, the individual organization's internet gateway, and the individual user's anti-spam filters. These technological defences – which lead to the creation of 'black' and 'white' lists of e-mail marketers – are the key barriers now faced by any organization attempting legitimately to use e-mail marketing as part of its marketing mix. And e-mail marketing works, but it only works for reputable companies if they comply with the law and apply best practice. Your target customers have to trust you if they are going to put you on their e-mail marketing 'white list'. These are all good reasons for the ISMS to deal effectively with both inbound and outbound e-mail marketing.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

The E-Government Act, signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), required each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by any other agency, contractor, or other source.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996, explicitly emphasized a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB) requires executive agencies within the federal government to:

- plan for security;
- ensure that appropriate officials are assigned security responsibility;
- periodically review the security controls in their information systems;
- authorize system processing prior to operations and, periodically, thereafter.

Contractual obligations

This clause of ISO27001 also covers contractual requirements. The Payment Card Industry Data Security Standard (PCI DSS) is an example of the type of security requirements that corporations might have to adopt as a result of contractual commitments, and therefore as part of organizational context and the baseline security controls. The five main payment card brands (Visa, MasterCard, Amex, JCB and Discover) collaborated on the development of a security standard (the PCI DSS) that they required all their merchants to accept, implement and provide evidence of successful compliance. The PCI requirements map to the controls of ISO/IEC 27001.

Intellectual property rights

Control 15.1.2 of ISO27002 says the organization should implement appropriate procedures to ensure compliance with legal restrictions on the

use of material to which intellectual property rights (IPR) might apply and on the use of proprietary software products.

Organizations deal with all sorts of third-party material, some of which may contain IPR in the form of copyright, design rights or trademarks. The CDPA is the cornerstone of copyright law in the United Kingdom. In the United States, the lay reader could begin an appreciation of the complexities of the subject by reference to the FAQs available from the United States Copyright Office (www.copyright.gov (archived at https://perma.cc/96BY-JTRN)) and the US Patent and Trademark Office (www.uspto.gov (archived at https://perma.cc/EJR5-HNYP)) and by reference to the DMCA itself: www.copyright.gov/legislation/dmca.pdf (archived at https://perma.cc/Y8H9-XEVF).

Copyright infringement can lead to legal action even involving criminal proceedings if there has been a clear breach, in the United Kingdom, of the CDPA or, in the United States, of the DMCA. Organizations should therefore adopt appropriate controls to avoid this happening. There are, broadly speaking, three controls that might be adopted.

The first is educational – ensuring that everyone in the organization understands the issues and takes action to avoid copyright infringement. Such an approach would require everyone to understand where the boundary between legal and illegal copying lies and what the requirements are, for instance, for identifying sources of information contained in new publications.

The second is simply to ban anyone in the organization from using any material that was not developed within the organization. This, while keeping the slate very clean, might be unnecessarily limiting, and the organization has to decide, in the light of a risk assessment, what its best course will be.

The third is to acquire appropriate licences from one or more of the licensing bodies that were described earlier in this chapter.

Software copyright

A most important issue in dealing with copyright is for the organization to ensure that it is not infringing the copyright of the suppliers of the software that it is using. Any software that is running on the organization's network is potentially subject to copyright restrictions, and it is essential for the organization to ensure that it has the correct type and number of licences for this software.

There are two types of user licence. The first is known as a 'per seat' licence; the second is for 'concurrent users'. 'Per seat' requires there to be a

licence for every installation, or instance, of the software. Typically, Microsoft Office licences, for instance, are supplied on this basis. 'Concurrent user' allows for a maximum number of simultaneous users and is more normal for shared software, such as some database applications. This enables the client software to be installed on as many machines as is wished, but typically the server software is set so that it will not allow more than the licensed number of users to work simultaneously. Different software packages are licensed on different bases, and the organization needs to be clear how each of its software packages is licensed and that it has paid for the correct number of licences.

There is also a wide range of 'freeware' available on the internet, which is software that can be downloaded subject to specific licence terms. It includes plug-ins such as Real Player, Macromedia Flash, etc. As these usually cannot be downloaded without the user accepting the licence conditions, there are not usually any licence-tracking issues here, although the organization ought to maintain a register of all such licences so as to ensure that their terms are being complied with. Wikipedia maintains a useful comparative list of open source licence terms at https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses (archived at https://perma.cc/49GU-A8VV).

Organizations need to maintain a register of software licences that lists all the licences they own as well as the purchase dates and, where appropriate, the disposal dates. Whenever a new PC is purchased, or added to the network, the register should be updated to reflect any additional software purchased or installed, and this requirement should be built into the change management documentation.

The organization should include in the access agreement signed by each member of staff before he or she is allowed to access any organizational computer a statement that only licensed and formally approved software may be used on the organization's computers and that any use of illegally obtained or unlicensed software will lead to disciplinary action. The organization will have to decide how to handle the wide range of freeware and shareware that is available across the internet. A risk assessment is the appropriate way to do this; maintaining a ban on the installation of freely downloadable software may be sensible, though it may not be cost-effective. This risk assessment needs to consider that allowing anyone to download whatever they want may result in non-business-related programs (including spyware and adware) appearing on the network and taking up valuable time, bandwidth and storage capacity. If these programs are then circulated

internally by e-mail, they could potentially cause a system crash as a result of system overload. This would be a security incident, as data required by the organization to pursue its objectives might become unavailable.

On a regular basis, the network administrator should carry out an audit of the software that is actually installed on the network PCs. This should be conducted at least annually, but experience shows that (particularly in fast-changing or growing networks) this could usefully be done as often as every quarter. These audits can be carried out by centralized network administration software, and while this will deal with permanently connected PCs, it will be necessary to ensure that all notebooks are scanned on a regular basis as well. Records should be kept of these audits, demonstrating that all machines have been audited and showing what action, if any, has been taken to remove illegal software (or acquire additional licences where necessary) and to deal with offenders.

The Federation Against Software Theft (FAST – www.fast.org (archived at https://perma.cc/Z8MK-Y2FS)) was set up in 1984 by the British Computer Society's Copyright Committee. It was the first software copyright organization. It has concentrated on raising the awareness of software piracy and lobbying Parliament for changes to the Copyright Act 1956 to reflect the needs of software authors and publishers. It represents both software publishers and end users and has a long history of working with both sides of the copyright relationship to ensure that software is properly managed. Corporations can join FAST, which provides a range of services designed to assist them to manage software properly and to comply with the law. FAST offers advice, assistance and training; it also offers an audit certificate that recognizes that the organization concerned is managing its software properly. This certificate is not required for the achievement of ISO27001, but the membership services may be of benefit to organizations that have very complex and extensive software set-ups and, perhaps, a background of inadequate management in this area. FAST says that there are many forms of software theft including:

'Professional counterfeits – look the same as genuine boxed products

Quasi counterfeits – try to look like the genuine product but usually fail in the presentation

CD compilation disks – several programs copied onto one disk

Hard disk loaders – dealers who load a copy of software onto hardware but do not supply disks, licences, manuals and Certificates of Authenticity, etc

Markets/Computer fairs – individuals selling obvious copies of computer programs

Peer to peer/IRC – individuals sharing software on the internet

Original equipment manufacturer (OEM) irregularity – software sold without a licence or the necessary hardware

Internet sites – downloading/uploading illegal software and utilities, downloading legitimate freeware and shareware in breach of the licence

Unlicensed corporate use – number of installations exceeds number of licences, number of users able to access software on a server exceeds the number of licences, software transferred from one company to another outside terms of the licence, installation of employees' own software onto company devices, different company name on opening screen etc.'

Anyone in the UK who decides to 'blow the whistle' on his or her employer for software infringement should be protected under the Public Interest Disclosure Act known as the 'Whistle Blowers Act'. This Act includes three basic requirements:

- The employee believes that his or her employer is committing a criminal offence or a breach of civil law. Under-licensing falls within both these categories. The illegal use of software in a business, and a manager turning a blind eye to misuse, are both criminal offences. Software infringement such as buying one copy and using many is a civil infringement.
- The employee must believe that the disclosure is 'substantially' true, act in good faith and not make any personal gain. The Act has regard to the identity of the person to whom the disclosure is made. A complaint to FAST would be reasonable, whereas employees seeking a fee from a newspaper might not be on such safe ground.
- The employee's disclosure was reasonable in all the circumstances. For instance, consideration should be given to whether the employee could have brought the matter to the attention of the company first without suffering detriment.

The implications of this should be clear for all organizations that are not already committed to complying with the existing software legislation. There is a very real risk that non-compliance will be exposed to FAST, to AAIPT or a similar organization, perhaps by a disgruntled current or former employee or competitor, with the potential consequences outlined above.

There are similar private organizations that are funded by the major software manufacturers to combat illegal use of software. They target organizations that they think may be using illegal software (which includes having more users of an off-the-shelf package than there are licences). There is no legal requirement to comply with their demands, and it is appropriate to take legal advice before responding to any demands that are made. It is always sensible, through the consistent application of an effective software copyright policy, to ensure that the organization is constantly able to demonstrate its compliance with the legislation and with the terms of any software licences.

Finally, organizations need to have an appropriate policy in place to deal with disposal of copyright material, which needs to be done in accordance with the licences.

Protection of organizational records

Control 18.1.3 of ISO27002 says the organization should protect its important records from loss, destruction or falsification. As ISO27002 explains, some records must be retained to meet statutory or regulatory requirements, while others may be needed to provide an adequate defence against potential civil or criminal action or to prove the financial status of the organization to the range of potential interested parties, including shareholders, tax authorities and auditors, and to meet contractual liabilities. Records do not have to (and should not) be kept forever, which can make it difficult to find what is required as and when it is required.

Therefore, time limits should be set for the retention of individual categories of information. After this time, records should be destroyed – in line with the procedure adopted by the organization to ensure that any confidential information within those records is not inadvertently made public. Some time limits will be set by statute or regulation, and the organization should establish, with its legal advisers, what the current categories of documents and retention requirements are. In the United Kingdom, HM Revenue & Customs requirements should also be met. Other categories and retention periods should be set to meet the requirements of interested parties. The picture is similar for most companies in their local jurisdictions and much more complicated for multinational companies, or organizations operating in more than one jurisdiction.

Due consideration should be given to the possible degradation of media over time, and any manufacturer's recommendations for storage should

obviously be followed. There may be implications, in change programmes, for data stored on – or only accessible through – media that are being replaced; adequate resources may need to be retained to access this information throughout its designated retention period, and the need for this should be assessed at the outset of any IT change plan.

Where paper archive facilities are to be used, it is important to consider not only the physical security of the premises but also how watertight they are and what their fire defences are like. Consideration should be given to what the back-up plan would be in the case of the archive facilities themselves being the subject of destruction. Storage should be carefully planned and carried out; individual cartons or boxes should be clearly marked as to their contents, the owners of the contents, the date of storage and the planned date of destruction.

There needs to be an indexing system that enables the storage box for individual documents to be quickly identified and documents retrieved. The retrieval and document return process also needs to be tightly controlled to ensure that a neat archive system does not break down through use, with documents becoming increasingly difficult to find. Ideally, the organization should appoint someone to be responsible for the maintenance of the archive, and there should be clearly documented procedures, within the ISMS, about how to use the archive and also a regular audit to ensure that the records are being maintained in accordance with the procedure.

These same principles (retention schedule, data inventory, appropriate protective controls and clear allocation of responsibility) should be applied to information stored digitally or on microfiche. Where organizations have more than one medium for storage, there should be a master index and guidelines for how each type of data should be treated. Where digital data storage vaults are to be deployed, the organization will need to ensure that the technology enables it to meet its data storage responsibilities cost-effectively.

ISO 15489–1 provides further information about managing organizational records, and, as it has been referenced by ISO27002, it would be worthwhile for any organization that has substantial record retention issues at least to be familiar with the guidance of this standard.

Privacy and protection of personally identifiable information

Control 18.1.4 of ISO27002 says the organization should develop and implement a data protection and privacy policy, applying controls to protect

personally identifiable information (PII) in accordance with relevant legislation. Within the United Kingdom, this primarily means compliance with the DPA and the Privacy and Electronic Communications Regulations, although organizations operating internationally or globally are likely to be subject to other legislation in other countries, particularly US legislation, as identified earlier in this chapter. In these circumstances, specialist legal advice should be taken.

The DPA was outlined at the beginning of this chapter, and the Information Commissioner should accept the certification of an organization's information security management system to ISO27001 as evidence that it does protect personal information in line with the legislation and applies 'appropriate security'. Registration with the Information Commissioner under the DPA is an absolute requirement, and there is no defence against a failure to do so, leaving an organization open to prosecution and fines.

Specific organizations, such as those processing high volumes of special categories of data, or those in the public sector, are legally required to appoint a data protection officer (DPO). The DPO can be either an employee or a contractor. Organizations that are not required to appoint a DPO will, given the complexity of the legislation and the potential liability, often do so. It is important to note that the GDPR forbids the appointment of DPOs that might have a conflict of interest; this tends to mean that those whose roles require them to determine the means and purposes of processing (such as, for instance, an information security manager) cannot also be the DPO.

In particular, organizations should be cognizant of the restrictions on transferring personal data to countries that are not within the European Union. This restriction is particularly important for organizations 'offshoring' any part of their customer support operations, or consolidating in a single location services previously delivered from multiple jurisdictions.

The EU–US Privacy Shield framework

This allows US corporations that are regulated by the Federal Trade Commission (FTC) and have operations in the EU to receive EU personal data. The Privacy Shield provides US organizations with a way to demonstrate a level of data protection that is not normally available under US Federal Law. The Privacy Shield compliance standards are certified through the Department of Commerce and enforced by the FTC; they are set out on the Commerce Department and FTC websites and carry Commerce Department certification. Only a small percentage of corporations have

met a requirement that enables them to obtain EU member state (one year renewable) permission to transfer data out of the European Union. More information on the safe harbor framework is at https://www.export.gov/safeharbor/eg_main_018236.asp (archived at https://perma.cc/3585-U2M4).

Regulation of cryptographic controls

Control 18.1.5 of ISO27002 says the organization should put in place controls to ensure compliance with any national agreements, laws, regulations or other requirements regarding the access to or use of cryptographic controls. This is because different countries have taken different steps to prevent the misuse of cryptography, including controls over the import and/or export of hardware and software that have cryptographic capabilities, or that could have such capabilities added, and requirements as to ways in which authorities should be able to access information encrypted by particular hardware or software. In the United Kingdom, relevant legislation includes the Electronic Communications Act 2000 (with the Electronic Signatures Regulations 2002 and the Electronic Commerce Regulations 2002) and the RIPA. There is also legislation that deals specifically with export/import restrictions on cryptography, including the Dual Use (Export Control) Regulations 2000.

Specialist legal advice should be taken to ensure that the organization is complying with the law as it currently stands, and where encrypted information or cryptographic equipment or controls are to be moved to another country, advice about that country should also be taken. It is worth considering, by means of a risk assessment, the costs and benefits of implementing such a security approach.

Compliance with security policies and standards

Control objective 18.2 requires the organization to ensure that its systems comply with its policies and standards and that the security of its information systems is regularly reviewed against the policies and technical standards laid down for them. Control 18.2.1, Independent review of information security, was addressed in Chapter 4, Organizing information security.

Compliance with security policy and standards

Control 18.2.2 of ISO27002 says the organization's managers should ensure that all security procedures within their areas of responsibility are carried out correctly; the organization also must ensure that all areas within the organization are subject to regular review to ensure that there is compliance with its documented security policies, procedures and standards. Clause 9.2 of ISO27001 ('Internal ISMS audits') sets out the broader requirement, and there should be a written procedure and an audit plan that describe how the audit process should be carried out. This will be essentially similar to an ISO9001 internal audit programme.

The first requirement is dealt with by including the responsibility for ensuring that security policies are complied with in the job description of all line managers. The real issue is for the organization to ensure that this is actually happening. The only effective way of ensuring management are doing their checks, as all ISO9001 organizations know, is through a programme of internal quality audits using appropriately trained staff or external consultants or other services providers. We recommend using the organization's own staff for this role, as internal auditing provides them with a good developmental opportunity – not only in the direct training in audit skills but in gaining an understanding of how different functions of the organization interact and how their processes work. Auditors' communication skills become highly developed and their profiles are raised as a consequence of interviewing staff at all levels of the organization.

One or more members of each department throughout the organization should be encouraged to volunteer for basic internal auditor training (which is usually offered by consultancies or companies that provide ISO27001 accredited certification audit services) and should then receive internally whatever additional training they will need. They will not need a significant level of technical skill or competence. They should be able to undertake this audit activity in addition to their normal work, and this responsibility should be added to their existing job descriptions.

Staff should not out audits of their own departments or of areas that are the responsibility of their own line manager; they can carry out audits of other areas within the organization. The organization will need to have in place a method for ensuring that it trains up enough auditors to cover staff turnover, holidays and other absence, planned or unplanned. The information security adviser should plan the audit schedule at least a year ahead, and in conjunction with the existing internal quality department, so as to

ensure that all areas are covered at least annually, that activities are coordinated and that there are no clashes or disruptions. A risk assessment might identify some areas as being in need of more frequent audit (the areas where the organization has most risk), and this should also be factored in.

Audits should be documented, with nonconformities identified in writing. Managers are expected to determine the cause of nonconformities, determine appropriate actions including the need to prevent recurrence, implement the decision and review its effectiveness. These action plans for rectification, together with dates and responsibilities, should be documented, and the information security adviser (or internal quality function) should have a system for ensuring that all due dates are achieved or otherwise followed up as appropriate. All nonconformities, together with action plans and status (ie showing which are closed and which not), should be reported to the regular meetings of the information security committee (see Chapter 4), together with an analysis of trends or assessment of larger threats that might not be immediately apparent at the individual incident level. These internally identified nonconformities and the results of corrective action should be available to external auditors when they carry out their review of the ISMS.

Sensibly, the nonconformities raised by any external auditor should be integrated into the organization system and receive numbers (usually in addition to the numbers given by the external auditor) that tie them into the existing continual improvement system for purposes of monitoring and analysis.

Technical compliance review

Control 18.2.3 of ISO27002 says the organization should regularly perform independent checks of its information systems to ensure that they comply with their documented security requirements and that the required hardware and software controls have been correctly implemented and maintained. This applies to network protection hardware and software (firewalls, routers) as well as to network resources (servers, user settings, access policies, etc). There should be a plan for these checks (which should be repeatable and documented) and they should be carried out as often as a risk assessment indicates is necessary. ISO/IEC 27008 provides guidance for auditing security controls. These checks should be carried out by someone who has the necessary technical skills and certainly not by those responsible for implementing the control in the first place.

Specialist assistance is required, and it can be obtained from any one of the security organization that has a security (penetration) testing offering. Some checking will have to be done manually by a trained tester; other checking can be done using automated software tools and the resulting reports can later be analysed by a trained tester. This type of checking includes intrusion or penetration testing of network defences. ISO27002 cautions that penetration testing should be carried out carefully, as it could lead to a system compromise. In practice, penetration testing has become one of the most important forms of technical compliance, as it identifies vulnerabilities that might be exploited by outside attackers.

A number of organizations should be approached with a schedule of the technical checking that will be required, and competitive prices obtained. References should be investigated thoroughly. The contract in place with any organization retained to do this sort of security checking should, of course, conform to the organizations standard requirements, and there should be particular consideration of how the contractor will be required to report vulnerabilities, so as to ensure that all that are detected are reported.

All nonconformities established under this process should be reported in accordance with the nonconformities procedure discussed earlier in this chapter and should be subject to the same level of monitoring, analysis and follow-up as any others.

Information systems audit considerations

Control 12.7.1 sets out how the organization should prepare for information systems audits (which might or might not) include technical compliance checking, as well as audits of, for example, licences and software installations. Essentially, says ISO27002, such audits should be scheduled so they don't interrupt business activity. In principle, of course, any audit interrupts business activity and therefore, the implementation of this control should be aimed at minimizing disruption and selecting periods of low or reduced activity and/or demand for carrying out any audit. Moreover, testing should be controlled, testers should preferably be limited to read-only access, and all testing logs should be controlled.

27

The ISO27001 audit

While some organizations might still debate the value of ISO27001 certification (arguing that what matters is the implementation of an effective ISMS rather than a badge), the market is moving against them, and a major objective of this book is to help those organizations that see the value in certification to be successful in achieving it. The first three chapters clearly explained all the benefits that accrue from a successful certification, and these will not be rehearsed here; a certification audit is a practical and cost-effective way of meeting the requirement in Control 18.2.1 for an independent review of information security, and provides a means of demonstrating compliance to ISO27001.

A certification audit will tend to use negative reporting (that is, it will identify inadequacies rather than adequacies) to assess an ISMS to ensure that its documented procedures and processes, the actual activities of the organization and the records of implementation meet the requirements of ISO27001 and the declared scope of the system. The outcome of the audit will be a written audit report (usually available soon after the completion of the audit) and a number of nonconformities and observations together with necessary corrective actions and agreed time-frames.

Selection of auditors

Chapter 3 touched on some of the issues that should be taken into account in selecting an ISO27001 certification body. Of course, any organization seeking certification will want to be sure that there is a cultural fit between itself and its supplier of certification services, and there will certainly be all the normal issues of ensuring that there is alignment between the desires of the buyer and the offering, including pricing and service, of the vendor.

It is completely appropriate to treat the selection of a certification body with the same professionalism as the selection of any other supplier.

There are three key issues that need to be taken into account when making this selection. The first is a general issue, the second is relevant to organizations that already have one or more externally certified management systems in place and the third applies specifically to organizations tackling ISO27001.

The first key point is that you should only use an accredited certification body (CB, also sometimes called a Registrar), one that is formally accredited by a National Accreditation Body that is a signatory to the International Accreditation Forum (IAF). These CBs deliver internationally recognized certification services, and their certificates are recognized as valid by all other IAF members; in other words, a UKAS-accredited certificate will be recognized as equivalent to a locally issued certificate accredited by another national accreditation body elsewhere in the world. There are a small number of unaccredited certification bodies offering combined consultancy and certification services outside the recognized international scheme; as they operate outside of the internationally recognized framework it is impossible to determine their competence, or extent of independence and hence the value to put on their certificates in terms of both assurance and credibility. Avoid them.

Secondly, it is essential that your ISMS is fully integrated into your organization; it will not work effectively if it operates outside of the management and operation of the organization or exists outside of and parallel to any other management systems.

Logically, this means that the framework, processes and controls of the ISMS must, to the greatest extent possible, be integrated with, for instance, your ISO9001 quality system; you want one document control system, one set of processes for each part of the organization, etc. Clearly, therefore, the certification body assessment of your management system must also be integrated: you want only one audit, which deals with all the aspects of your management system. It is simply too disruptive of the organization, too costly and too destructive of good business practice to have anything else. You should take this into account when selecting your ISO27001 certification body, and ensure that whoever you choose can and does offer an integrated assessment service. However, the fact that a CB is accredited to offer ISO9001 certification does not automatically mean it is accredited for ISO27001; you will need to check with the CB. If you are currently using a CB that is not accredited for ISO27001, you will have to consider switching to one that is able to offer certification to both standards.

The third issue that you should take into account when selecting your supplier of certification services is their approach to certification itself. An ISMS is fundamentally designed to reflect the organization's assessment of risks in and around information security. In other words, each ISMS will be different. It is important therefore that each external assessment of an ISMS takes that difference into account so that the client gets an assessment that adds value to its business (which includes positive feedback as well as non-conformities), rather than one that is merely a mechanical comparison of the ISMS against the requirements of ISO27001. Inquiring how a potential provider of ISO 27001 certification ensures its auditors are appropriately competent for your specific business is one means of helping ensure you receive a valuable service.

Once an accredited certification body has been selected and terms agreed (using the same basis of contracting as is applied to any other third-party supplier), the organization can turn to the actual process of certification. This process will be completely familiar to any organization that has already undergone certification to ISO9000 or any other management system standard. The certification body will want to go through an initial two-stage process. The first stage will be a Stage 1 audit, which enables the audit body to become acquainted with the organization, to carry out a document review, to assure themselves that the ISMS is sufficiently well developed to be capable of withstanding a formal audit and to obtain enough information about the organization and the intended scope of the certification to plan their Stage 2 audit effectively. This visit is usually relatively short and, depending on the size of the organization, may require only one or two days to carry out. The certification body will use this visit to ensure it has sufficient time and the appropriate competency profile in the audit team to successfully complete the Stage 2 audit, as well as to ensure that your organization is ready for that challenge.

Initial audit

The first formal audit, known as the initial audit, will usually take place over two stages. The audit process involves testing the organization's documented processes (the ISMS) against the requirements of the standard (Stage 1, a readiness review), to confirm that the organization has set out to comply with the standard, and then testing actual compliance by the organization with its ISMS (Stage 2, the implementation audit). The entire two-stage audit will follow a pre-ordained plan, and the auditors will have

communicated with whoever is their liaison point (usually the information security manager) about whom they will wish to interview and in what order they will want to do it. There is no defined maximum period between the Stage 1 and Stage 2 audits, although it is unusual for it to exceed three months. Some negotiation is possible here, but usually over timing and availability rather than subject matter.

Each audit will start and finish with a management meeting. The auditors, just like financial ones, will need a separate room for the duration of the audit and appropriate arrangements made for refreshments. Many audits will involve at least two auditors, who may have different areas of expertise. There will be a lead, or principal, auditor, who will be responsible for the overall progress of the audit. The organization being audited should ensure that its liaison is on hand to support the auditors throughout the process; this might include guiding auditors around the premises, introducing them to those staff next on their list to interview, and dealing with queries and issues arising.

At the end of each day, there will usually be a brief wrap-up meeting at which (usually) any areas of nonconformity with either the standard or the ISMS are identified. This part of the process will again be completely familiar to any organization that has gone through an ISO9001 certification. Nonconformities can be either minor or major; minor ones tend to vary in usefulness but major ones could very easily mean that the organization is not (at this stage) capable of successful certification. Often, upon identification of a major nonconformity the auditors will suggest that the audit process be suspended and started afresh once the organization has had time enough to address this major issue. This can be expensive and time-consuming, and have a negative effect on morale and the commitment within the organization to achieving certification.

There are two components to carrying out successful certification audits. The first is the level of preparedness of the organization's ISMS and the second is the way in which the employees of the organization are themselves prepared for the audit.

Preparation for audit

No audit can take place until sufficient time has passed for the organization to have in place a working internal audit and management review process and to demonstrate compliance with clause 10, the requirement for

improvement. In other words, auditors will be looking for evidence that the ISMS is continuing to improve, not merely that it has been implemented. This means that a period of time will have to elapse between completion of the implementation and commencement of audit. How long will depend on the complexity of the organization and its ISMS, but one should assume that there will need to be good progress with the first cycle of internal audits for all of the key processes and arrangements. (It is for the certification body to determine exactly what it requires in order to be convinced of the establishment, effectiveness and ongoing arrangements for internal ISMS audit and management review, aspects it is required to confirm prior to issuing a certificate, and hence possibly something worth asking when selecting your certification body.)

The level of preparedness for an audit should then be assessed by carrying out a comprehensive review. The detailed work should be carried out by the information security adviser and by the quality function, and this should all be reviewed by the management information security forum. A comprehensive review could use this book, starting with Chapter 4, and question the extent to which adequate steps have been taken to implement the various recommendations.

The Statement of Applicability (SoA) needs particularly detailed review. It should be possible to identify the extent to which each of the controls identified as necessary has been implemented and, where implementation has been only partial, to determine what steps (and how long they will take) will be necessary to complete its implementation. In particular, all instances in which the organization has chosen not to implement a recommended control should be reviewed in detail to ensure that this decision was appropriate, and that the justification for exclusion that is included on the SoA is sufficient. Similarly, all instances in which a control has been implemented to a greater or lesser extent than indicated as necessary by a proper information security risk assessment should be reviewed, and if it is not possible (too difficult, expensive, etc) to improve the level to which the control has been implemented, managers should formally accept the highest level of residual risk.

Once a comprehensive review has been completed and the management steering group is satisfied that the ISMS is complete, complies with the standard and has been adequately implemented (and at least one cycle of internal audits of key areas of the ISMS as identified by the risk assessment also needs to have been completed), then the organization can safely move on to the Stage 1 visit by its external auditors.

Preparation of staff within the organization, prior to the audit, as to what they might expect and how to handle auditors is also a valuable step. Staff should be taught that auditors should be treated with complete honesty, and direct answers should always be given, even if this requires admitting to a lack of knowledge or error. Equally, staff should be trained to answer the question asked by the auditor and not to provide more, or less, information than is required. Auditors will usually ask for an explanation as to how a particular component of the ISMS works and will then want to be shown. This is normal and is how the audit is conducted.

ISO27001 Assessments Without Tears (available from https://www.itgovernance.co.uk/shop/product/iso27001-2013-assessments-without-tears-a-pocket-guide-second-edition) provides useful advice to those that are likely to be interviewed by an auditor. ISO27007 and ISO27008 set out guidelines for the ISO27001 auditor on how to conduct an audit. They are valuable both to the organization's internal audit teams as part of their training and to the management information security forum so that they understand the approach that the auditors will take and can ensure that the organization is adequately prepared for the audit. The latter provides detailed guidance on auditing Annex A controls.

The outcome of the initial audit should, if the organization has diligently followed all the recommendations contained in this manual, be a positive recommendation for certification of the ISMS to ISO27001 and the issue of a certificate setting this out. The certificate should be appropriately displayed and the organization should start preparing for its first surveillance visit, which will take place about six to twelve months later. Any minor nonconformities should be capable of being closed out by mail, and any certificate issued will be dependent on this happening within an agreed timescale.

The certificate will refer to the latest version of the SoA and auditors will check for updates at their subsequent visits. Therefore, when supplying a copy of the certificate to clients, stakeholders or other parties, the organization should be prepared to provide a copy of the most recent SoA (whether controlled or otherwise). While the SoA is a living document, updated as and when necessary, the organization should endeavour to keep such updates and alterations to a minimum.

It is possible that the issued accredited certificate mentions international and national standards from which information security contols in the SoA have been selected, such as ISO27017 and/or ISO27018.

Terminology

It is worth noting that different accredited certification bodies use different terms to describe what are, without wishing to imply a preference or endorsement of any one option, simply major and minor nonconformities. Some of the descriptors currently in use are shown in Table 27.1.

TABLE 27.1 Terms used by different accredited certification bodies for major and minor nonconformities

Major	Minor
major nonconformity	minor nonconformity
category 1 nonconformity	category 2 nonconformity
nonconformity	issue
major nonconformity	nonconformity

Not all CBs will raise nonconformities at the Stage 1 audit; some will make 'findings', which should nevertheless be dealt with through your nonconformity and corrective action process like any nonconformity.

While variations in use of terminology is obviously annoying, given that the accredited certification bodies work in the field of standardization, this inconsistency needs to be acknowledged for other reasons. With the increasing use of ISO27001-accredited certification in the supply chain, we will no doubt see these terms being used to specify reporting requirements, measure conformance and compare organizations. Obviously, unless the terminology is clearly defined for such applications, it could lead to meaningless comparisons.

Appendix 1

Useful websites

IT Governance Ltd

www.itgovernance.co.uk (archived at https://perma.cc/52C6-BA5J)

Comprehensive library of ISO27001 books, tools and resources
www.itgovernance.co.uk/iso27001 (archived at https://perma.cc/5Z44-FFHT)

Blogs
www.alancalderitgovernanceblog.com (archived at https://perma.cc/Y9WY-KKKQ)
http://blog.itgovernance.co.uk (archived at https://perma.cc/KSG9-6246)

ISO27001 certification-related organizations

United Kingdom Accreditation Service
www.ukas.com (archived at https://perma.cc/PBP9-55AX)

BSI
www.bsigroup.com (archived at https://perma.cc/ERJ8-N2JA)

Bureau Veritas Quality International (BVQI)
www.bureauveritas.co.uk (archived at https://perma.cc/87K2-XPQJ)

DNV GL – Business Assurance
www.dnvgl.com/about/business-assurance/index.html (archived at https://perma.cc/RU25-CU34)

Lloyd's Register Quality Assurance (LRQA)
www.lr.org/en (archived at https://perma.cc/X8CY-86LH)

NQA Certification
www.nqa.com (archived at https://perma.cc/Z6LN-GX2Q)

SGS
www.sgs.com (archived at https://perma.cc/9WRJ-FBVL)

Microsoft

www.microsoft.com (archived at https://perma.cc/GX4A-BB7A)
www.microsoft.com/download (archived at https://perma.cc/UH3M-5EKJ)

Microsoft Security Centre
https://www.microsoft.com/en-gb/security (archived at https://perma.cc/YY9A-6W65)

Information security

(UK) Alliance Against Intellectual Property Theft
www.allianceforip.co.uk (archived at https://perma.cc/Y5KH-RNNT)

Anti-phishing Working Group
www.antiphishing.org (archived at https://perma.cc/3BMD-EW2H)

British Computer Society
www.bcs.org (archived at https://perma.cc/F2JT-8CR9)

Carnegie Mellon Software Engineering Institute
www.sei.cmu.edu (archived at https://perma.cc/7GK6-8FMN)

Carnegie Mellon Software Engineering Institute Computer Emergency Response Team (CERT) Coordination Centre
www.sei.cmu.edu/about/divisions/cert/index.cfm (archived at https://perma.cc/C9ZJ-KUQ7)

Centre for Education and Research in Information Assurance and Security
www.cerias.purdue.edu (archived at https://perma.cc/Q2UU-JXBG)

(UK) Centre for the Protection of National Infrastructure
www.cpni.gov.uk (archived at https://perma.cc/3M6L-NUES)

Common Vulnerabilities and Exposures
https://cve.mitre.org (archived at https://perma.cc/ZS35-2RNV)

CWE/SANS Top 25 Most Dangerous Software Errors
http://cwe.mitre.org/top25/ (archived at https://perma.cc/T6SQ-JVHF)

Computer Security Resource Center (US National Institute of Standards and Technology)
csrc.nist.gov (archived at https://perma.cc/Z5WL-42XB)

ENISA
www.enisa.europa.eu (archived at https://perma.cc/Q2UU-JXBG)

(US) Federal Computer Emergency Readiness Team
www.us-cert.gov (archived at https://perma.cc/RV7C-QS8M)

(UK) Federation Against Software Theft
www.fast.org (archived at https://perma.cc/Z8MK-Y2FS)

Forum of Incident Response and Security Teams
www.first.org (archived at https://perma.cc/K8T8-7LSK)

GCHQ, Cheltenham
www.gchq.gov.uk (archived at https://perma.cc/RF95-WKDY)

HMG Cabinet Office Security Policy
www.gov.uk/government/publications/security-policy-framework (archived at https://perma.cc/MB7X-SHGA)

(UK) Information Commissioner
www.ico.org.uk (archived at https://perma.cc/6BTV-VF5H)

Information Systems Audit and Control Association
www.isaca.org (archived at https://perma.cc/M2SL-RC7N)

Information Systems Security Association
www.issa.org (archived at https://perma.cc/9QKG-VRYE)

(UK) INFOSEC Exhibition
www.infosecurityeurope.com/ (archived at https://perma.cc/CN6T-DPNR)

Institute for Applied Network Security
www.iansresearch.com (archived at https://perma.cc/Q2J9-AC58)

Institute of Internal Auditors, North America
na.theiia.org (archived at https://perma.cc/5384-BNTF)

(UK) Intellectual Property Office
www.gov.uk/government/organisations/intellectual-property-office
(archived at https://perma.cc/J6EG-3ZL2)

International Information Systems Security Certification Consortium
www.isc2.org (archived at https://perma.cc/8SL2-F4SU)

Internet Engineering Task Force (IETF)
www.ietf.org(archived at https://perma.cc/WQ56-M5UM)

Internet Security Alliance
www.isalliance.org (archived at https://perma.cc/74Z2-U9RP)

Internet Watch Foundation
www.iwf.org.uk (archived at https://perma.cc/VUM2-HCZB)

OWASP Top Ten
www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (archived
at https://perma.cc/SE24-2276)

PCI DSS
www.pcisecuritystandards.org (archived at https://perma.cc/6WAP-EMUQ)

(US) Privacy Rights Clearinghouse
www.privacyrights.org (archived at https://perma.cc/7S5N-U4AP)

SANS Institute
www.sans.org (archived at https://perma.cc/A85T-VFFU)

Search Security
https://searchsecurity.techtarget.com (archived at https://perma.cc/
QH3R-YGQB)

Security Week
www.securityweek.com (archived at https://perma.cc/46PW-BT6E)

Vigilance: The security magazine
www.vigilance-securitymagazine.com (archived at https://perma.cc/FRU8-PGLT)

Virus Bulletin
www.virusbulletin.com (archived at https://perma.cc/GU93-J6GX)

Appendix 2

Further reading

The following list of books and standards may be of interest to the business manager who wants a more detailed understanding of specific security issues or aspects of ISMS implementation.

Readers should bear in mind that the nature of security threats and the appropriate responses (particularly those provided by technology) are changing all the time. Chapter 4 identified a number of ways in which the reader can remain current with the security world and these should be implemented. The websites identified in Appendix 1 are also good sources of relevant information.

ISO27000 family of standards includes:

ISO/IEC 27000:2018 (ISO 27000) – ISMS overview and vocabulary

ISO/IEC 27001:2013 (ISO 27001) – ISMS requirements

ISO/IEC 27002:2013 (ISO 27002) – Code of practice for information security controls

ISO/IEC 27003:2017 (ISO 27003) – ISMS implementation guidance

ISO/IEC 27004:2016 (ISO 27004) – Information security metrics and measurements

ISO/IEC 27005:2018 (ISO 27005) – Information security risk management

ISO/IEC 27006:2015 (ISO 27006) – Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2017 (ISO 27007) – Guidelines for information security management systems auditing

ISO/IEC 27008:2011 (ISO 27008) – Guidelines for auditors on information security controls

ISO/IEC 27011:2016 (ISO 27011) – Guidelines supporting the implementation of information security management (ISM) in telecommunications organizations

ISO 27799:2008 (ISO 27799) – Guidelines for managing information security in the health sector

Information about, and copies of, these standards are available from https://www.itgovernance.co.uk/iso27000-family (archived at https://perma.cc/32TC-KEN6). This web page is also updated whenever a new standard in this family is published, and contains regularly updated information about those ISO27000 standards that are still under development.

Books

IT Governance Publishing is the leading publisher of books about information security management, all of which are available through specialist booksellers, online retailers and in softcover, eBook and audio formats from the company's own website at www.itgovernancepublishing.co.uk (archived at https://perma.cc/CQP3-U3NN)

Calder, A (2013) *ISO27001/ISO27002: A Pocket Guide*, 2nd edn, IT Governance Publishing, Ely, UK

Calder, A (2013) *The Case for ISO27001*, 2nd edn, IT Governance Publishing, Ely, UK

Calder, A (2016) *Nine Steps to Success: An ISO27001 implementation overview*, 3rd edn, IT Governance Publishing, Ely, UK

Calder, A (2016) *Selling Information Security to the Board*, 2nd edn, IT Governance Publishing, Ely, UK

Calder, A (2018) *Network and Information Systems (NIS) Regulations: A pocket guide for digital service providers*, IT Governance Publishing, Ely, UK

Calder, A (2018) *Network and Information Systems (NIS) Regulations: A pocket guide for operators of essential services*, IT Governance Publishing, Ely, UK

Calder, A (2018) *NIST Cybersecurity Framework: A pocket guide*, IT Governance Publishing, Ely, UK

Calder, A and Watkins, S (2019) *Information Security Risk Management for ISO27001/ISO27002*, IT Governance Publishing, Ely, UK

Calder, A and Williams G (2019) *PCI DSS: A pocket guide*, 6th edn, IT Governance Publishing, Ely, UK

Drewitt, T (2013) *A Manager's Guide to ISO22301*, IT Governance Publishing, Ely, UK

Honan, B (2014) *ISO27001 in a Windows Environment*, 3rd edn, IT Governance Publishing, Ely, UK

Kouns, B and Kouns, J (2011) *The Chief Information Security Officer: Insights, tools and survival skills*, IT Governance Publishing, Ely, UK

Krausz, M (2014) *Information Security Breaches: Avoidance and treatment based on ISO27001*, 2nd edn, IT Governance Publishing, Ely, UK

Krausz, M (2015) *Managing Information Security Breaches: Studies from real life*, 2nd edn, IT Governance Publishing, Ely, UK

Mehan, J E (2014) *CyberWar, CyberTerror, CyberCrime, Cyber Activism*, IT Governance Publishing, Ely, UK

Mehan, J (2016) *Insider Threat: A guide to understanding, detecting, and defending against the enemy from within*, IT Governance Publishing, Ely, UK

Mooney, T (2015) *Information Security: A practical guide – Bridging the gap between IT and management*, IT Governance Publishing, Ely, UK

Roer, K (2015) *Build a Security Culture*, IT Governance Publishing, Ely, UK

Simmons, A (2015) *Once More Unto the Breach: Managing information security in an uncertain world*, 2nd edn, IT Governance Publishing, Ely, UK

Ticher, P (2018) *Data Protection and the Cloud: Are you really managing the risks?* 2nd edn, IT Governance Publishing, Ely, UK

Viira, T (2018) *Lessons Learned: Critical information infrastructure protection – How to protect critical information infrastructure*, IT Governance Publishing, Ely, UK

Vladimirov, A, Gavrilenko, K and Michajilowski, A (2015) *Assessing Information Security: Strategies, tactics, logic and framework*, 2nd edn, IT Governance Publishing, Ely, UK

Watkins, S (2013) *An Introduction to Information Security and ISO27001*, IT Governance Publishing, Ely, UK

Watkins, S (2013) *ISO27001 Assessments without Tears*, 2nd edn, IT Governance Publishing, Ely, UK

Wright, C (2016) *Fundamentals of Information Security Risk Management Auditing: An introduction for managers and auditors*, IT Governance Publishing, Ely, UK

Zinatullin, L (2016) *The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour*, IT Governance Publishing, Ely, UK

Other books worth reading include:

Mitnick, K D and Simon, W L (2005) *The Art of Intrusion: The real stories behind the exploits of hackers, intruders and deceivers*, Wiley Publishing, Indianapolis

Mitnick, K D, Simon, W L and Wozniak, S (2003) *The Art of Deception: Controlling the human element of security*, Wiley Publishing, Indianapolis

Schneier, B (2015) *Secrets and Lies: Digital security in a networked world*, Wiley Computer Publishing, New York

Tipton, H F (2016) *Information Security Management Handbook*, 6th edn, vol 6, Auerbach Publications, Boca Raton, FL

Toolkits

Documentation toolkits are a collection of customizable templates written by industry experts to help you produce documentation that meets the requirements of your chosen management system standard, compliance or certification project. The following toolkits, published by IT Governance Publishing, are designed to help organizations implement an ISMS:

ISO27001 2013 ISMS Standalone Documentation Toolkit

ISO 22301 BCMS Documentation Toolkit

EU General Data Protection Regulation (GDPR) Documentation Toolkit

Data Security and Protection (DSP) Toolkit Documentation Templates

PCI DSS Documentation Compliance Toolkit

vsRisk Cloud

vsRisk Cloud is an online tool for conducting an information security risk assessment aligned with ISO 27001. It is designed to streamline the process and produce accurate, auditable and hassle-free risk assessments year after year.

INDEX

access control (and) 161–77
  hackers: prime motivations and techniques 161–66 *see also* hackers
  Network Access Control 169–77 *see also subject entry*
  policy 167–69
  system configuration 166–67
advanced persistent threat (APT) 17
Annex A controls 110
  A/ISO27002 control set 106
annual loss expectancy (ALE) 95, 96
articles/papers *see* NIST
asset management 139–56
  acceptable use of assets 143–44
  asset owners 139–40
  government classification markings 148–49 *see also* United Kingdom
  information classification 144–46
  information labelling and handling 150–55
    SEC1 *and* legal disclaimer example 151–52
    SEC2 material controls 152–53
    SEC3 material safeguards 154–55
  information lifecycle 149–50
  inventory: customer relationship management (CRM) data *and* types of asset 140–43
  non-disclosure agreements (NDAs) and trusted partners 155–56
    and asset handling procedures 156
  unified classification markings: SEC1, SEC2 *and* SEC3 146–48
auditing standards
  No.5 (AS No.5) 30
  No.12 *Identifying and assessing risks of material misstatement* 31
auditors (and)
  external ISO27001 65
  internal auditor courses: ISO27001 *and* Foundations of Information Security Management 74

Basel 2/3 1, 22
  Frameworks 90
BS7799 38–39, 42

business continuity management system (BCMS) 335–36
business and information continuity management (and) 323–37
  business continuity and risk assessment (and) 325–26
    maximum tolerable period of disruption (MTPD) 325
    recovery time objective (RTO) 325
  the business continuity management process 324–25
  business continuity planning framework 328–32
    documentation of critical assets and access information 332
    documentation of individual responsibilities 332
    emergency procedures 331
    escalation procedure 329–30
    external mobilization and briefing procedure 330
    fall back procedures, advance planning of 331
    internal mobilization and briefing procedure 330
    resumption procedures 331
    staff and personnel training in BCPs 332
    temporary operational procedures 331
    testing of plans, timing and frequency of 131–32
    the same format for individual BCPs 330–31
  developing and implementing continuity plans (and) 327–28
    ISO/IEC 27031 Code of Practice 328
    planning process 327–28
  information security continuity (and) 335–37
    effectiveness of information security continuity plans (control 17.1.3) 337
    establishment of documented procedures (control 17.1.2) 336–37
    information security continuity objectives (control 17.1.1) 336

ISO27002 control objective 335–36
redundancy in information systems (control 17.1.4) 337
ISO22301 *and* developing a business continuity plan (BCP) 323–24
testing, maintaining and reassessing business continuity plans 332–35
and change management 335
scenarios for use in 334–35
business loss, categories of 103
business-to-business (b2b) 10, 277
e-commerce propositions 5
business-to-consumer (b2c) 5, 278
BYOD (bring your own device) issues 115, 118

Calder, A 92
CERT (Computer Emergency Response Team) 71, 306, 307
coordination centre 167
CHAP (Challenge Authentication Protocol) 180
COBIT (Control Objectives for Information and Related Technologies) 43, 60, 232
commercial off-the-shelf (COTS) software 249, 274, 294
communications management 253–57 *see also* network security management
compliance (and) 339–64 *see also* legislation (EU), legislation (UK) *and* legislation (US)
Control 18 339
e-commerce 339
identification of applicable legislation (and) 340–53
code of practice 349
contractual obligations 353
Network and Information Security Directive (EU) 349
information systems audit considerations 364
intellectual property rights (and) 353–58 *see also* copyright *and* FAST
copyright infringement 354
software copyright 354–58
'whistleblowers' 357
privacy and protection of personally identifiable information 359–61
protection of organizational records 358–59
regulation of cryptographic controls 361
with security policies and standards 361–64
Computer Security Resource Center (US National Institute of Standards and Technology) 72
copyright 127, 128, 263, 270, 298, 342, 347, 353–58 *see also* legislation (UK)
and British Computer Society's Copyright Committee 356 *see also* FAST
infringement 354
software 354–58
Copyright Licensing Agency (CLA) 347
the Corporate Governance Code (and) 25–28
key questions for board to ask 27–28
listed companies 26
Risk Guidance (paragraph 24) 28
Risk Guidance (paragraphs 24, 26, 27) 25–26
principle C2: on internal control 25
section A.1: on role of the board *and* risk management 25
the Corporate Governance Code, the FRC Risk Guidance *and* Sarbanes–Oxley 23–35
the Combined Code 23–24 *see also* reports
the Corporate Governance Code 25–28 *see also subject entry*
enterprise risk management 31–33 *see also subject entry*
IT governance 34–35
regulatory compliance 33–34 *see also* legislation (UK) *and* legislation (US)
Sarbanes–Oxley 29–31, *30 see also subject entry*
the Turnbull Report 24–25 *see also subject entry*
COSO: Committee of Sponsoring Organizations of the Treadway Commission 90
and ERM framework 30, 31–33
Crime-as-a-Service (CaaS) business model 15
Critical National Infrastructure (CNI) 16–17
Cruise, T (in character of Ethan Hunt) 206
cryptography (and) 197–203
digital signatures 200–201
encryption 198–99
asymmetric/public key 199

symmetric *and* Data Encryption Standard (DES) 198
key management 202–03
and risk assessment process questions 202–03
non-repudiation services 201–02
policy statement 197–98
public key infrastructure 199–200
see also legislation (UK)
Cryptolocker 243
customer relationship management (CRM) systems *and* assets 142–43
cybercrime (and) 14–15
cyber attacks 7
cyber security 5
Cybercrime Convention (Council of Europe) 15
organized crime groups (OCGs) 15

data breaches 11, 12, 14
demilitarized zones (DMZs) of extranets 173, 256
development and support processes (and) 285–94
secure development environment 289–90
and outsourced development 290
secure development policy (and) 285–88
restrictions on changes to software packages 288
system change control procedures *and* PRINCE2 286–87
technical review of applications after operating platform changes 288
vulnerabilities (OWASP Top 10) 285–86
secure systems engineering principles 289
security and acceptance testing (and) 290–94
measures to be implemented 292–93
Microsoft 291–92
protection of test data 294
system acceptance testing (control A.14.2.9) 291
Systems Development Lifecycle (SDLC) 285

Economic Co-operation and Development, Organisation for (OECD) 3
and *Principles of Corporate Governance* (1999) 3
enterprise risk management *and* COSO ERM framework (and) 31–33
definition of ERM 32
eight components of COSO ERM framework 32
equipment security (and) 217–28
cabling security *and* ISO27002 measures 222–23
clear desk and clear screen policy 227–28
equipment maintenance; risk assessment *and* insurance 223
equipment siting and protection 217–20
see also ISO27002
removal of assets 224
secure disposal or reuse of equipment 225–27
and unattended user equipment 226–27
security of equipment and assets off-premises (and) 224–25
encryption, staff training, risk assessments *and* insurance 224–25
supporting utilities *and* uninterruptible power supply (UPS) 220–22
European Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention) 348
European Union (EU) *see also* legislation (EU)
cyber security strategy (2013): 'An Open, Safe and Secure Cyberspace' 16
EU–US Privacy Shield registration 297
information classification scheme 148
Europol *and* Internet Organised Crime Threat Assessment (iOCTA) 15
exchanges of information (and) 259–72
agreements on information transfers 262–63
e-mail policy 265–66
e-mail security risks (ISO27002) 264–66
e-mail and social media 263–64
information transfer policies and procedures 259–62
measures to be taken 260–62
internet acceptable use policy 269–71
misuse of the internet (and) 266–69
acceptable use policy (AUP) 267–69
negative publicity from employee dismissals 267
recreational surfing 267
reduction in employee productivity 267
surf control technology *and* acceptable use policy (AUP) 267–68

social media 271–72
spam 266

FAST (Federation Against Software Theft) 356, 357 *see also* copyright
and forms of software theft 356–57
Financial Reporting Council (FRC)
Risk Guidance 22, 28, 38, 90
and Sarbanes–Oxley 38 *see also* legislation (US)
further reading (Appendix 2) 379–83

Guidelines on Firewalls and Firewall Policy (NIST, Special Publication 800–41) 175

hackers (and) 161–66
Certified Ethical Hacker (CEC) certification 162
prime motivations: challenge, mischief, working around *and* theft 161
'script kiddies' 162
techniques 162–66
human resources security (and) 121–37
disciplinary process 134–35
during employment (and) 128–34
e-learning 129–30
training/training needs analysis (TNA) 131–34
user-specific training 131
using intranet or SharePoint 133–34
job descriptions and competency requirements 121–23
screening *and* verification (control 7.1.1 of ISO27002) 123–26
termination or change of employment 135–37 *see also* control areas
terms and conditions of employment *and* control 7.1.2 (ISO27002) 126–28
confidentiality agreement 126–28
non-disclosure agreement (NDA) 127–28
review of agreements 127–28

IBITGQ Internal Audit qualification 74–75
information classifications
SEC1 147–48, 151–52
SEC2 147–48, 152–53, 155
SEC3 147–48, 154–55
information security management systems (ISMSs) 5–6, 60–61, 78
documentation 210
information security policy and scope (and) 77–87
context of the organization 77–78
costs, the monitoring of progress *and* key points for reviewing progress 86–87
information security policy 78–84
key questions: what? where? who? *and* why? 79–84
policy statement 85–86
information security – why is it necessary? (and) 9–22 *see also* surveys
advanced persistent threat (APY) 9, 17
benefits of an information security management system 22
cybercrime 14–15 *see also subject entry*
cyberwar 16–17
future risks 17–20
impacts of information security threats 13–14
information insecurity 12–13 *see also* reports
legislation 20–21 *see also* legislation (UK) *and* legislation (US)
the nature of information security threats (and) 10–12 *see also* reports
risk categories: damage to operations, to reputation *and* legal damage 11–12
Information Security Risk Management for ISO28001/ISO27002 92 *see also* Calder, A *and* Watkins, S G
Information Systems Security Certification Consortium (ISC2) 70
Infosecurity Today Magazine 72
International Electrotechnical Commission 40
International Organization for Standardization (ISO, Geneva) 40
introduction (and/and the) 1–8
book as key resource – six reasons for 1–2
definition of IT governance 3–4
information economy 2–3
information security 4–8 *see also* ISO27001
ISACA *and* ISC2 professional organizations 72
ISC Common Body of Knowledge (CBK) 97
and five types of control 97
ISMS (and)
requirements 229
Sharepoint 229
social media 271–72

ISMS standard (and) 6–7, 92, 99–100, 101, 150, 169
Clause 6.1.2 91
Documentation Toolkit 86
ISO27001 ISMS Lead Auditor 74
meaningful 100
scope 96, 99–100
structuring and development of an effective 144
ISO Directives for standardization 47, 48
ISO9000 229, 231
ISO9001 58
certificated quality management system 47
certified management system 48
ISO15489–1 on managing organization records 359
ISO20000 47, 231
ISO22301 47, 231, 323–24, 335
ISO27000 93, 231
definition of 'external context' 77
definitions for key terms used in security policy 82–83
family of standards 106
ISO27001 (and) 95, 96, 99, 100, 106, 109, 171, 173, 215, 229, 231, 231, 233–34, 253, 275, 301, 335, 367
2013 68
auditor/audit 72, 74, 93, 175, 206
British Computer Society (BCS) as link for 70
certificate 107
certification 108
clause 5.2 86
clause 7.2 63
clause 9.2: internal ISMS audits 362
concept of cross-functional forum disappeared from 61
contractual requirements 353
control A.6.1.1 66
control A.6.1.3 73
implementation 47–48
ISMS 92
ISMS Documentation Toolkit 86
ISMS lead Auditor 74
key issues 69–70
as outcome-orientated management standard 113
project 69
project group 62–68 *see also* organizing information security
risk assessment 91
and Risk Owner (at 6.1.3.f) 111
risk treatment plan 89
ISO27001 audit (and) 365–71
Assessment Without Tears 370
initial audit 367–68
preparation for 368–70
and Statement of Applicability (SoA) 369
selection of auditors for 365–67
terminology 371
ISO27001 standards 2, 6, 7–8, 34, 35, 37–54, 57, 58, 231, 233–34 *see also* ISO/IEC27000 series of standards
benefits of certification 37–38
clause 5.3 55
clause 9.2e – control A.6.1.2 for segregation of duties 59
clause 9.3 – requirement for management review of ISMS 58
continual improvement and metrics 53–54
continual improvement, Plan–Do–Check–Act, and process approach 43–44
and note on numbering 44
documentation (for) 48–53
change management 51–52
communication *and* compliance with clause 7.4 52–53
ISO27001 ISMS Documentation Toolkit 50
leadership 50
reviews 53
history of ISO27001 and ISO27002 38–40
ISO27001-focused certified training courses 69
management system integration 47–48
Microsoft certification 99
structured approach to implementation 44–47 *see also* Plan–Do–Check–Act
and implementation issues 46–47
use of the standard 41–42
ISO27002 99, 109, 150, 173, 194, 254, 284, 308–09, 316
at 10.1.1: on policy on use of cryptographic controls 197
advice on selection and design of secure areas 211
best practice on deployment of software 249–50
email security risks 264
software development 233
on consideration of additional controls for secure areas 231–232

Clause 5 79
Clause 5.1 86
Clause 8.1.2 (Ownership of Assets) 66
Clause 8.2.1 144
Clause 12.1.4 233
Clause 12.2.1: measures to limit risk of malware infection 245–48
Clause A.6.1.1 55
controls to reduce e-mail security risks 263
controls/specific controls recommended 208, 211–12, 235–38
measures for cabling security 222–23
measures for equipment siting and protection 117–20
recommendation on media handling 157
recommendations for user registration process 181–84
on review of normal access rights 187
Section 7 of 121
Section 16 of 310
steps to protect program source libraries
ISO27002 standard
maintenance of information process equipment (control 11.2.4) 223
numbering sequence 44
ISO27002:2013 106
ISO27003 standard: formal guidance on ISMS implementation 56, 57, 81
ISO27005 96
guidance 103
ISO27017 106
ISO27018 106
ISO27033 series of standards 253
ISO27035 point of contact (PoC) 313
ISO31000 92
ISO/IEC27000 series of standards 40–41
ISO/IEC27000 2, 60
ISO/IEC27001 key standard 2, 353
ISO/IEC27001:2013 6, 7, 8, 30, 31, 41, 108
clause 9.1 requirement for evaluation information security performance and effectiveness of ISMS 112
ISO/IEC27002 106
and Code of Practice 42–43
ISO/IEC27002:2013 6
ISO/IEC27005 92
ISO/IEC27017 99
ISO/IEC27018 99
ISO/IEC27035 Code of Practice for incident management 310
ISO/IEC27036 295
IT governance
definition of 3
strategies: specific drivers for adoption by organizations 3–4
ITIL approach to IT service management 43, 60, 232, 286, 295, 306

legislation (EU)
General Data Protection Regulation (GDPR) 21, 297, 340
Network and Information Security Directive 349
Privacy Directive (2003) 340
legislation (UK)
Bribery Act 341
Companies Act (2004) 26–27
Companies Act (2006) 21, 266, 340
Computer Misuse Act (CMA, 1990) 14–15, 21, 33, 341, 345–46
reviewed mid-2004 by All Party Internet Group (APIG) 346
updated by the Police and Justice Act (2006) 21, 346
Copyright Act (1956) 88, 340, 356
Copyright, Designs and Patents Act (CDPA, 1988) 21, 340, 346–47
list of legislation amending 347
on corporate goverance 341
Crime and Security Acts 341
Data Protection Act (DPA, 2018) 21, 33, 294, 340, 342–43, 344
Electronic Commerce Regulations (2002) 347
Electronic Communications Act (2000) 198, 200, 341, 347–48
Electronic Signatures Regulations (2002) 347
Environmental Information Regulations (2004, 2005) 345
Freedom of Information Act (FOIA, 2000) 341, 344–45
Human Rights Act (HRA, 1998) 307, 341, 348
Money Laundering Regulations (2003) 341
Police and Justice Act (2006) 21
Clauses 35–38 346
Privacy and Electronic Communications Regulations (2003, 2011) 33, 341, 344
Proceeds of Crime Act (2002) 341
Public Interest Disclosure Act ('Whistle Blowers Act') 357

Regulation of Investigatory Powers Act (2000) 307, 341, 348
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000) 348–49
Terrorism Act (2000) 341
Waste Electrical Equipment regulations 226
legislation (US)
201.CMR.17: Massachusetts law protecting personal information 350
Californian Senate Bill 1386 342
CAN-SPAM Act 342
provisions enforced by the Federal Trade Commission (FTC) 352
Consumer Privacy Act (California) 342
data breach laws 342
and EU-US Safe Harbor regulations 33
Fair Credit Reporting Act (FCRA, 1999) 341, 352
Federal Information Security Management Act (FISMA, 2002) 33–34, 342, 353
Gramm–Leach–Bliley Act (GLBA) 33, 341 *and* Final Rule 351
Health Insurance Portability and Accountability Act (HIPAA) 33, 341, 350
and HITECH Act (2009) 351
Information Technology Management Reform Act (1996) 353
and list of state data breach laws 350
Millennium Digital Copyright Act 342
Online Privacy Protection Act (OPPA, 2004: California) 342
Paperwork Reduction Act (1995) 353
Patriot Act 342
Sarbanes–Oxley Act (SOX, 2002) 1, 22, 29–31, 33, 341 *see also subject entry*
SEC Regulation FD *and* rule 17 a-4 341
Lobban, Sir I 16

Manningham-Buller, E 16
media handling 157–60
disposal of media 158–59
management of removable media 157–58
physical media in transit 159–60
Microsoft 72, 279–80, 291–92
Active Directory 181
certification 99
Safety & Security Centre 71
security website 306
software 249
software, service packs and patches 291
systems 181
technet 71
vulnerabilities and guidelines 166–67
Windows: baseline measures for server security 281–82
website: www.microsoft.com 71
Mission Impossible 206
mobile devices 115–20 *see also* teleworking
mobile computing 115
and Wired Equivalent Privacy (WEP) 117
monitoring and information security incident management 305–21
assessment of/decision on information security events 318
incident management – responsibilities and procedures 310–13
events likely to be classified as incidents 311
formal control of action for recovery/correction of system failures 312–13
incident response procedure/contingency planning process 311–12
information security events and incidents 310
legal admissibility 321
logging and monitoring 305–10
administrator and operator logs 308
clock synchronization 309–10
event logging/fault logs 305–07
monitoring system use 307–08
protection of log information 308
reporting information security events 313–16
reporting software malfunctions *and* steps for reporting procedure 316–18
and reporting security weaknesses 317–18
response to information security incidents 318–21
collection of evidence 320–21
learning from incidents 319–20

NATO classification system *and* NATO information classification scheme 147, 148
Network Access Control (and) 169–77

access to networks and network services 173–74
extranets 170–71
firewalls and network perimeter security 174–75
network intrusion detection systems (NIDS) 176–77
NIST Publication SP 800–31: *Intrusion Detection Systems* 177
routers and switches 175–76
Special Publication 800–47, Security Guide for Interconnecting Information Technology Systems 171
user authentication for external connections 177
virtual private networks (VPNs) 170
wireless networks 171–73
network security management (and) 253–57
security of network services 255–56
segregation in networks 256–57
NIST 106, 306
Guidelines on Firewalls and Firewall Policy (800–41) 175
Intrusion Detection Systems (SP 800–31) 177
paper on SDLC 285
Security for Telecommuting and Broadband Communications (SP 800–44) 118
Systems Development Lifecycle (SDLC) 285
website 175

OHSAS 18001 standard 47
operations security (and) 229–38
back-up *and* ISO27002 – controls to be considered 235–38
back-up of critical paper files 237
definition and application of retention period for business information 238
minimum level of back-up information 236
recovery and restoration procedures 237
Redundant Array of Independent Disks (RAID) 237–38
regular testing of back-up media 236–37
same levels of security as original data 236
change management (and) 231–33
capacity management 232–33
change control procedure 232
documented operating procedures 229–31
separation of development, testing and operational environments 233–34
organizing information security (and) 55–75
contact with authorities 73
contact with special interest groups 71–73
the cross-functional management forum 61–62
independent review of information security 74–75
the information security manager 59–61
defined and key activities for 60–61
information security in project management 73–74
internal organization *and* ISO27002, ISO27003 56–58
the ISO27001 project group 62–68
allocation of information security responsibilities 66–68
chairperson 64–65
members 62–64
records 65–66
management review 58
segregation of duties 70–71
specialist information security advice 68–70
summary 75

password(s) (and) 6, 15, 67, 137, 163, 164–65, 168, 176, 179–81, 183, 186–89 192, 225, 226–27, 234, 280, 283–84
authentication technology protocols: TACACS+ *and* RADIUS 180
management system 193–94
Password Authentication Protocol (PAP) 180
Payment Card Industry Data Security Standard (PCIDSS) 275, 282, 283, 353
PCAOB's Auditing Standard No. 5 35
replaced AS No 2 in 2007 35
physical and environmental security (for) 205–15
and A.11 control category 205
delivery and loading areas 214–15
ISO27002: measures to be considered 215
secure areas 205–14
physical entry controls 208–10

physical security perimeter 205–08
protecting against external and environmental threats 212–13
securing offices, rooms, facilities *and* keys 210–12
working in secure areas 213–14
Plan–Do–Check–Act (PDCA) 43, 44
cycle for ISMS 112
Public Company Accounting Oversight Board (PCAOB) 37
public key infrastructure (PKI) 199
standard X.509 199

qualitative risk analysis 96–98
assets within the scope 96
controls 97–98
impacts 97
risk assessment 97
threats 96
vulnerabilities 96–97

reports
Cadbury Report 23
on corporate governance and directors' remuneration (Cadbury *and* Greenbury) 23
Verizon Data Breach Investigations Report 12
Verizon Data Breaches Report 11, 14
risk assessment and Statement of Applicability 89–113
Cyber Essentials scheme (UK) 99–105
identify assets 100–101
identify criticality: relationships between assets and objectives 101–03
identify potential threats and vulnerabilities (likelihood) 103–05
establishing security requirements 89
gap analysis 109–10
measures of effectiveness 112–13
risk assessment tools 110–11 *see also subject entry*
risk treatment plan 111–12
risks, impacts and risk management 89–99 *see also subject entry*
selection of controls and Statement of Applicability (SoA) 106–07
Statement of Applicability (SoA) Example 108–09
introduction 108
as specified: clause 6.1.3.d to ISO/IEC 27001:2013 108
the Statement (SoA) 108–09, *109*
risk assessment tools: VS Risk™ (Vigilant Software Ltd) 110, 141 *see website*
risks, impacts and risk management 89–99
approach to risk assessment 91–93
identify the boundaries 98–99
linked objectives for risk management plans 90
qualitative risk analysis 96–98 *see also subject entry*
quantitative risk analysis 95–96
risk acceptance criteria 90–91
who conducts information security risk assessment? 93–95

Sarbanes–Oxley Act (SOX, 2002) 1, 22, 29–31, 90
internal controls and audit 29–31, *30 see also* ISO/IEC27000 series of standards
secure areas 213–14
security breaches (Target, 2013) 14
Security Policy Framework: SPF (UK) 148–49
levels of classification/protective marking 148–49
Security Wire Digest 247
SMART (specific, measurable, achievable, realistic, time-bound) objectives 101
social media, risks and ISMS control 271–72
Statement of Applicability (SoA) 107, 108–09, *109*, 195
supplier relationships 295–303
addressing security within supplier agreements 297–99
and issues for particular consideration 298–99
ICT supply chain 299–301
security 300–301
information security policy for supplier relationships 295–97
managing changes to supplier services 302–03
monitoring and review of supplier services *and* key responsibilities 301–02
surveys (on)
CBI Cybercrime (2001) 20
Global State of Information Security Survey (PricewaterhouseCoopers, 2018) 9
Information Security Breaches Survey, UK:(managed by PwC): key findings 12

from OECD economies 12–13
US State of Cybercrime (CSO Magazine, US Secret Service, Software Engineering Institute [CERT Division] *and* PwC) 14
system acquisition, development and maintenance 273–84
e-commerce issues (and) 275–78
Application Service Management 277
non-repudiation – of origin, submission *and* receipt 276–77
risk from hackers 276
protecting application services transactions 283–84
securing application services on public networks 274–75
security requirements analysis and specification 273–74
security technologies 278–81
internet protocol security (IPSec) 280
PKIX working group of IETF 280
Secure Electronic Transaction (SET) protocol 281
Secure Multipurpose Internet Mail Extensions (S/MIME) 280
secure sockets layer (SSL) 279–80
server security 281–82 *see also* Microsoft
server virtualization *and* information security risks 282–83
system and application access control 191–95
access control to program source code 195
information access restriction (control A.9.1.1) 191–92
password management system 193–94
secure log-on procedures 192–93
use of privileged utility programs 194–95
Systems Development Lifecycle (SDLC) 285 *see also* NIST

tables
Sarbanes–Oxley Act (SOX, 2002): high-profile and critical sections *30*
Statement of Applicability (SoA) table *109*
teleworking (and) 118–20
controls, risk assessment and formal policy within ISMS 118
plans/procedures to authorize/control activities (ISO27002, Control 6.2.2) 118
Security for Telecommuting and Broadband Communications (NIST) 118
Turnbull Report – 'Internal Control: Guidance for directions on the Combined Code' 24–25
principles of internal control adopted by UK government 27

United Kingdom (UK) *see also* legislation (UK) *and* Security Policy Framework: SPF (UK)
Accredited Certification Scheme 42
ACPO Good Practice Guide for Digital Evidence 121
Authors' Licensing and Collecting Society (ALCS) 347
Centre for the Protection of National Infrastructure: WARP toolbox 320
Combined Code (1998) 23–24
Copyright Licensing Agency (CLA) 347
Corporate Governance Code 21, 23, 24, 26, 38
Cyber Essentials scheme 99
FRC Risk Guidance (formerly Turnbull Guidance) 1, 26
HM Revenue & Customs 358
HMG Security Policy Framework 34
Intellectual Property Office 347
national security strategy (2015): cyber risk as Tier 4 national security risk 16
'Orange Book': *Management of Risk – Principles and concepts* 27, 37
Publishers Licensing Society (PLS) 347
Trade and Industry, Department of 38
United Nations: classification system 147
United States (US) *see also* legislation (US) *and* surveys
Copyright Office 354
data breach reporting laws 21
development of a National Office of Cyberspace 350
EU–US Privacy Shield registration 297
ratification of Cybercrime Convention (2006) 15
Secret Service 12 *see also* reports
security classification scheme 149
UPS (uninterruptible power supply) 220–21

useful websites (Appendix 1) 373–77
user access management (and) 179–89
establishing authenticity of users *and* user identification 179–80
user access provisioning 184–89
management of privileged access rights 185–86
management of secret authentication information 186–87 *see also* ISO27002
review of user access rights 187–88
use of secret authentication information *and* password rules 188–89
user registration and deregistration 181–84 *see also* ISO27002

VLANs (Virtual LANs) 256
and VPN technology 256
voice over IP (VoIP) technology 173

WARP (Warning, Advice and Reporting Point) 71
Watkins, S G 92
Wikipedia: classification systems *and* government classification schemes 146, 148
wireless networks 171–73
802.11 standards group 172
Bluetooth 172–73
security standards WPA *and* WPA2 172
Wired Equivalent Privacy (WEP) (and) 172