Correction for incorrect response to exercise

Chapter 2, page 37 question 5: the answer is A (not B as per the answer given on page 230).
BCS, THE CHARTERED INSTITUTE FOR IT

BCS, The Chartered Institute for IT, is committed to making IT good for society. We use the power of our network to bring about positive, tangible change. We champion the global IT profession and the interests of individuals, engaged in that profession, for the benefit of all.

Exchanging IT expertise and knowledge
The Institute fosters links between experts from industry, academia and business to promote new thinking, education and knowledge sharing.

Supporting practitioners
Through continuing professional development and a series of respected IT qualifications, the Institute seeks to promote professional practice tuned to the demands of business. It provides practical support and information services to its members and volunteer communities around the world.

Setting standards and frameworks
The Institute collaborates with government, industry and relevant bodies to establish good working practices, codes of conduct, skills frameworks and common standards. It also offers a range of consultancy services to employers to help them adopt best practice.

Become a member
Over 70,000 people including students, teachers, professionals and practitioners enjoy the benefits of BCS membership. These include access to an international community, invitations to a roster of local and national events, career development tools and a quarterly thought-leadership magazine. Visit www.bcs.org/membership to find out more.

Further information
BCS, The Chartered Institute for IT,
First Floor, Block D,
North Star House, North Star Avenue,
Swindon, SN2 1FA, United Kingdom.
T +44 (0) 1793 417 424
F +44 (0) 1793 417 444
(Monday to Friday, 09:00 to 17:00 UK time)
www.bcs.org/contact
http://shop.bcs.org/
CONTENTS

Figures and tables vii
Authors viii
Acknowledgements x
Abbreviations xi
Preface xvi

1. INFORMATION SECURITY PRINCIPLES 1
   Concepts and definitions 1
   The need for, and benefits of, information security 9
   Sample questions 17

2. INFORMATION RISK 19
   Threats to, and vulnerabilities of, information systems 19
   Risk management 24
   Sample questions 36
   References and further reading 37

3. INFORMATION SECURITY FRAMEWORK 39
   Organisation and responsibilities 39
   Organisational policy, standards and procedures 47
   Information security governance 53
   Information assurance programme implementation 58
   Security incident management 63
   Legal framework 67
   Security standards and procedures 79
   Sample questions 85
   References 87

4. SECURITY LIFE CYCLES 88
   The information life cycle 88
   Testing, audit and review 90
   Systems development and support 93
   Sample questions 100
   Reference 101

5. PROCEDURAL AND PEOPLE SECURITY CONTROLS 102
   General controls 102
   People security 104
   User access controls 109
| CONTENTS |
|------------------|-----|
| Training and awareness | 117 |
| Sample questions | 123 |

### 6. TECHNICAL SECURITY CONTROLS 125
- Technical security | 125
- Protection from malicious software | 126
- Networks and communications | 132
- Operational technology | 144
- External services | 147
- Cloud computing | 153
- IT infrastructure | 158
- Sample questions | 164

### 7. PHYSICAL AND ENVIRONMENTAL SECURITY 166
- Physical security | 166
- Different uses of controls | 174
- Sample questions | 175

### 8. DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT 177
- Relationship between DR/BCP, risk assessment and impact analysis | 177
- Resilience and redundancy | 179
- Approaches to writing plans and implementing plans | 180
- The need for documentation, maintenance and testing | 182
- Need for links to managed service provision and outsourcing | 184
- Need for secure off-site storage of vital material | 185
- Need to involve personnel, suppliers and IT systems providers | 186
- Relationship with security incident management | 187
- Compliance with standards | 188
- Sample questions | 188

### 9. OTHER TECHNICAL ASPECTS 190
- Investigations and forensics | 190
- Role of cryptography | 194
- Threat intelligence | 202
- Conclusion | 206
- Sample questions | 206
- References and further reading | 207

### APPENDIX A 209
- Activity solution pointers | 215
- Sample question answers | 230
- Glossary | 233
- Index | 241
FIGURES AND TABLES

Figure 2.1  The risk management life cycle  26
Figure 2.2  A typical risk matrix  27
Figure 4.1  The data and information life cycle  89
Figure 6.1  The Plan–Do–Check–Act model  144
Figure 9.1  Symmetric key encryption  196
Figure 9.2  Asymmetric key encryption  198
Figure 9.3  Producing a signed message digest  199
Figure 9.4  Verifying message integrity  200

Table 2.1  One possible rating framework for risk assessment  31
Andy Taylor, after initially teaching in secondary schools, Andy has been involved with information assurance for over 35 years, starting when he served in the Royal Navy in several posts as security officer. He had responsibility for all classified and cryptographic materials in both warships and shore establishments, at times helping to maintain the effectiveness of the nuclear deterrent. After leaving the Royal Navy, he chose a further career in consultancy and was instrumental in achieving one of the first accreditations for a management consultancy against the information security standard ISO 17799 (now ISO/IEC 27001). As an independent information security consultant, he has provided information assurance advice to a wide variety of organisations in the public and private sectors including the Health Service, Home Office, utility regulators, the Prison and Probation Services and web developers. He has developed and delivered a number of specialist security briefings to help educate users in the effective use of information in a secure manner, and has provided induction security training in many organisations. He has been directly involved with the development, establishment and maintenance of several different certification schemes relating to information security including the assessment of individuals and of training. He is a Fellow of both BCS and the Association for Project Management (APM), a Chartered IT Professional and a member of the Chartered Institute of Information Security. He has a passionate interest in maintaining the highest standards of information assurance and helping others to gain expertise in it.

David Alexander has over 20 years’ experience in the field of information security. He has an MSc in Information Security from Royal Holloway, University of London and specialises in advanced network security, information security architectures, cryptographic protocols and the security of operational technology/industrial control systems. He is Senior Security Architect for the Urenco Group. David has worked on the design and assurance of critical national infrastructures around the world and has wide experience of commercial, central government and defence projects. Involved in IT for over 30 years, the first 10 in mainstream IT before he changed sides from ‘poacher to gamekeeper’. David is a Fellow of BCS and of the Chartered Institute of Information Security, and a Chartered Security Architect and IT professional. He was also one of the first people in the world accredited as Lead Auditor for what is now ISO/IEC 27001, a certification he has maintained through all the versions. As well as working for Urenco, David teaches the Network Security module on the Royal Holloway Information Security MSc programme.
Amanda Finch is the CEO of the Chartered Institute of Information Security and has specialised in information security management since 1991. She has always been an active contributor to the industry and for many years has been dedicated to working towards the discipline being recognised as a profession. Over her career she has been engaged in all aspects of information security management and takes a pragmatic approach to the application of security controls to meet business objectives. Through her work she has developed an extensive understanding of the commercial sector and its particular security needs. In her current role she works with industry, government and academia, assisting all sectors in raising levels of competency and education. Amanda has worked within the retail and banking sectors as well as with the Information Security Forum. She has a Masters degree in Information Security, holds full membership of the Chartered Institute of Information Security with Founder status, and is a Fellow of BCS. In 2007 she was awarded European Chief Information Security Officer of the Year by Secure Computing magazine and is frequently listed as one of the most influential women within the industry.

David Sutton’s career spans more than 50 years in information and communications technology, incorporating radio transmission, international telephone switching, mainframe computing and data networking. At Telefónica O2 UK he was responsible for ensuring the continuity and restoration of its core cellular networks, and he represented the company in the UK electronic communications industry’s national resilience forum. In December 2005 he gave evidence to the Greater London Authority enquiry into the impact of the 7/7 London bombings on mobile telecoms. Since retiring from O2, David has undertaken a number of critical information infrastructure projects for the European Network and Information Security Agency (ENISA), and has developed training material on business continuity and information risk management for InfoSec Skills in addition to authoring books on information security and business continuity. He has been a member of the BCS Professional Certification Information Security Panel since 2005 and a tutor on the distance learning Information Security MSc course at Royal Holloway, University of London. He is a member of the Chartered Institute of Information Security, a Fellow of BCS and a Chartered IT Professional.
ACKNOWLEDGEMENTS

For this third edition, we would like to thank Ian Borthwick for his help in getting this updated edition into print. The cartoons were originally drawn by Ed Brown, so our continuing thanks go to him. We would also like to thank colleagues and clients, families and friends who willingly, or more usually unwittingly, have provided many of the anecdotes, examples and stories with which we have tried to explain some of the principles in this book.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>2FA</td>
<td>two-factor authentication</td>
</tr>
<tr>
<td>4G</td>
<td>International Mobile Telecommunications Advanced or LTE Advanced</td>
</tr>
<tr>
<td>5G</td>
<td>fifth generation cellular network telephony</td>
</tr>
<tr>
<td>ACL</td>
<td>access control list</td>
</tr>
<tr>
<td>ACPO</td>
<td>Association of Chief Police Officers (UK)</td>
</tr>
<tr>
<td>ADSL</td>
<td>asymmetric digital subscriber line</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>BCP</td>
<td>business continuity plan</td>
</tr>
<tr>
<td>BCS</td>
<td>British Computer Society, The Chartered Institute for IT</td>
</tr>
<tr>
<td>BIA</td>
<td>business impact analysis</td>
</tr>
<tr>
<td>BS</td>
<td>British Standard</td>
</tr>
<tr>
<td>BYOD</td>
<td>bring your own device</td>
</tr>
<tr>
<td>CA</td>
<td>certification authority</td>
</tr>
<tr>
<td>CAI</td>
<td>computer aided instruction</td>
</tr>
<tr>
<td>CAPS</td>
<td>Certified Assisted Products</td>
</tr>
<tr>
<td>CAS</td>
<td>Independent Evaluation for Assured Services (UK NCSC)</td>
</tr>
<tr>
<td>CASB</td>
<td>cloud access security broker</td>
</tr>
<tr>
<td>CBT</td>
<td>computer-based training</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria (certificate)</td>
</tr>
<tr>
<td>CC ITSEC</td>
<td>Common Criteria for Information Technology Security Evaluation Criteria</td>
</tr>
<tr>
<td>CCP</td>
<td>Certified Cyber Professional</td>
</tr>
<tr>
<td>CCRA</td>
<td>Common Criteria Recognition Arrangement</td>
</tr>
<tr>
<td>CCTV</td>
<td>closed-circuit television</td>
</tr>
<tr>
<td>CEH</td>
<td>Certified Ethical Hacker (qualification)</td>
</tr>
<tr>
<td>CERT</td>
<td>computer emergency response team</td>
</tr>
<tr>
<td>CESG</td>
<td>Communications-Electronics Security Group (largely superseded by UK’s NCSC)</td>
</tr>
<tr>
<td>CFO</td>
<td>chief finance officer</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CIISec</td>
<td>Chartered Institute of Information Security</td>
</tr>
<tr>
<td>CIO</td>
<td>chief information officer</td>
</tr>
<tr>
<td>CISMP</td>
<td>Certificate in Information Security Management Principles</td>
</tr>
<tr>
<td>CISO</td>
<td>chief information security officer</td>
</tr>
<tr>
<td>CiSP</td>
<td>Cyber Security Information Sharing Partnership</td>
</tr>
<tr>
<td>CLEF</td>
<td>Commercial Licensed Evaluation Facility</td>
</tr>
<tr>
<td>CMM</td>
<td>Capability Maturity Model</td>
</tr>
<tr>
<td>CoCo</td>
<td>code of connection</td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organizations of the Treadway Commission</td>
</tr>
<tr>
<td>COTS</td>
<td>commercial off-the-shelf</td>
</tr>
<tr>
<td>CPA</td>
<td>Commercial Product Assurance</td>
</tr>
<tr>
<td>CPNI</td>
<td>Centre for the Protection of National Infrastructure</td>
</tr>
<tr>
<td>CREST</td>
<td>Council of Registered Ethical Security Testers</td>
</tr>
<tr>
<td>CRO</td>
<td>chief risk officer</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Alliance</td>
</tr>
<tr>
<td>CTAS</td>
<td>CESG Tailored Assurance Service</td>
</tr>
<tr>
<td>CTCPEC</td>
<td>Canadian Trusted Computer Product Evaluation Criteria</td>
</tr>
<tr>
<td>CTI</td>
<td>cyber threat intelligence</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures database</td>
</tr>
<tr>
<td>DCMS</td>
<td>Department for Digital, Culture, Media and Sports</td>
</tr>
<tr>
<td>DCS</td>
<td>distributed control system</td>
</tr>
<tr>
<td>DDoS</td>
<td>distributed denial of service</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>dynamic host configuration protocol</td>
</tr>
<tr>
<td>DHS</td>
<td>Department for Homeland Security</td>
</tr>
<tr>
<td>DMZ</td>
<td>demilitarised zone</td>
</tr>
<tr>
<td>DNS</td>
<td>domain name system</td>
</tr>
<tr>
<td>DoS</td>
<td>denial of service</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>DR</td>
<td>disaster recovery</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data Rates for GSM Evolution</td>
</tr>
<tr>
<td>EDI</td>
<td>electronic data interchange</td>
</tr>
<tr>
<td>EDS</td>
<td>ETSI documentation service</td>
</tr>
<tr>
<td>EFTA</td>
<td>European Free Trade Association</td>
</tr>
<tr>
<td>eIDAS</td>
<td>Electronic Identification, Authentication and Trust Services</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Network and Information Security</td>
</tr>
<tr>
<td>EPC</td>
<td>European Patent Convention</td>
</tr>
<tr>
<td>ERP</td>
<td>enterprise resource planning</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FAIR</td>
<td>Factor Analysis of Information Risk</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCA</td>
<td>Financial Conduct Authority</td>
</tr>
<tr>
<td>FIPS PUBS</td>
<td>Federal Information Processing Standards Publications</td>
</tr>
<tr>
<td>FIRST</td>
<td>Forum for Incident Response and Security Teams</td>
</tr>
<tr>
<td>FoIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FSA</td>
<td>Financial Services Act</td>
</tr>
<tr>
<td>GATT TRIPS</td>
<td>General Agreement on Tariffs and Trades, Trade Related Aspects of Intellectual Property Rights</td>
</tr>
<tr>
<td>GCHQ</td>
<td>Government Communications Headquarters</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GFS</td>
<td>Grandfather-Father-Son</td>
</tr>
<tr>
<td>GIAC</td>
<td>Global Information Assurance Certification</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm-Leach-Bliley Act</td>
</tr>
<tr>
<td>GPEN</td>
<td>GIAC Penetration Tester (qualification)</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications standard (2G)</td>
</tr>
<tr>
<td>HIDS</td>
<td>host intrusion detection system</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HRA</td>
<td>Human Rights Act</td>
</tr>
<tr>
<td>HSDPA</td>
<td>High-Speed Downlink Packet Access</td>
</tr>
<tr>
<td>HTTP(S)</td>
<td>hypertext transfer protocol (secure)</td>
</tr>
<tr>
<td>IA</td>
<td>information assurance</td>
</tr>
<tr>
<td>IaaS</td>
<td>infrastructure as a service</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>ICS</td>
<td>industrial control system</td>
</tr>
<tr>
<td>ICT</td>
<td>information communications and technology</td>
</tr>
<tr>
<td>ID&amp;A</td>
<td>identification and authentication</td>
</tr>
<tr>
<td>IDC</td>
<td>inter-domain connector</td>
</tr>
<tr>
<td>IDS</td>
<td>intrusion detection system</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IIISP</td>
<td>Institute of Information Security Professionals</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange protocol</td>
</tr>
<tr>
<td>IM</td>
<td>instant messaging</td>
</tr>
<tr>
<td>IoC</td>
<td>indicator of compromise</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>intellectual property</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IPR</td>
<td>intellectual property rights</td>
</tr>
<tr>
<td>IPS</td>
<td>intrusion prevention system</td>
</tr>
<tr>
<td>IPSec</td>
<td>internet protocol security</td>
</tr>
<tr>
<td>IRT</td>
<td>incident response team</td>
</tr>
<tr>
<td>IS</td>
<td>information systems</td>
</tr>
<tr>
<td>ISDN</td>
<td>integrated services digital network</td>
</tr>
<tr>
<td>ISF</td>
<td>Information Security Forum</td>
</tr>
<tr>
<td>ISMS</td>
<td>information security management system</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Information Technology Security Evaluation Criteria</td>
</tr>
<tr>
<td>ITT</td>
<td>invitation to tender</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LTE</td>
<td>long term evolution (see also 4G)</td>
</tr>
<tr>
<td>LOB</td>
<td>line of business</td>
</tr>
<tr>
<td>MFA</td>
<td>multi-factor authentication</td>
</tr>
<tr>
<td>MiFID</td>
<td>Markets in Financial Instruments Directive</td>
</tr>
<tr>
<td>MPLS</td>
<td>multi-protocol layer switching</td>
</tr>
<tr>
<td>NCA</td>
<td>National Crime Agency</td>
</tr>
<tr>
<td>NCSC</td>
<td>National Cyber Security Centre (part of GCHQ)</td>
</tr>
<tr>
<td>NDA</td>
<td>non-disclosure agreement</td>
</tr>
<tr>
<td>NIDS</td>
<td>network intrusion detection system</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Systems directive</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Centre</td>
</tr>
<tr>
<td>NPCC</td>
<td>National Police Chiefs’ Council</td>
</tr>
<tr>
<td>OCTAVE</td>
<td>Operationally Critical Threat, Asset and Vulnerability Evaluation</td>
</tr>
<tr>
<td>OES</td>
<td>operator of essential services</td>
</tr>
<tr>
<td>OOB</td>
<td>out of band</td>
</tr>
<tr>
<td>OSA</td>
<td>Official Secrets Act</td>
</tr>
<tr>
<td>OSCP</td>
<td>Offensive Security Certified Professional (qualification)</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Source Intelligence</td>
</tr>
<tr>
<td>OT</td>
<td>operational technology</td>
</tr>
<tr>
<td>OTP</td>
<td>one-time password</td>
</tr>
<tr>
<td>PaaS</td>
<td>platform as a service</td>
</tr>
<tr>
<td>PABX</td>
<td>private automatic branch exchange</td>
</tr>
<tr>
<td>PACE</td>
<td>Police and Criminal Evidence Act</td>
</tr>
<tr>
<td>PAS</td>
<td>Publicly Available Specification</td>
</tr>
<tr>
<td>PCBCM</td>
<td>Practitioner Certificate in Business Continuity Management</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PCIRM</td>
<td>Practitioner Certificate in Information Risk Management</td>
</tr>
<tr>
<td>PDCA</td>
<td>Plan–Do–Check–Act</td>
</tr>
<tr>
<td>PenTest</td>
<td>penetration test</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PII</td>
<td>personally identifiable information</td>
</tr>
<tr>
<td>PIN</td>
<td>personal identification number</td>
</tr>
<tr>
<td>PKI</td>
<td>public key infrastructure</td>
</tr>
<tr>
<td>ProtMon</td>
<td>protective monitoring</td>
</tr>
<tr>
<td>RDSP</td>
<td>relevant digital service provider</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>RIPA</td>
<td>Regulation of Investigatory Powers Act</td>
</tr>
<tr>
<td>ROI</td>
<td>return on investment</td>
</tr>
<tr>
<td>SaaS</td>
<td>software as a service</td>
</tr>
<tr>
<td>SABSA</td>
<td>Sherwood Applied Business Security Architecture</td>
</tr>
<tr>
<td>SANS</td>
<td>Sysadmin, Audit, Network, Security</td>
</tr>
<tr>
<td>SCADA</td>
<td>supervisory control and data acquisition</td>
</tr>
<tr>
<td>SIEM</td>
<td>security information and event management</td>
</tr>
<tr>
<td>SLA</td>
<td>service level agreement</td>
</tr>
<tr>
<td>SOC</td>
<td>security operations centre</td>
</tr>
<tr>
<td>SOMA</td>
<td>Security Operations Maturity Architecture</td>
</tr>
<tr>
<td>SSL</td>
<td>secure sockets layer</td>
</tr>
<tr>
<td>SSO</td>
<td>single sign on</td>
</tr>
<tr>
<td>TCSEC</td>
<td>Trusted Computer System Evaluation Criteria</td>
</tr>
<tr>
<td>TLS</td>
<td>transport layer security</td>
</tr>
<tr>
<td>ToE</td>
<td>target of evaluation</td>
</tr>
<tr>
<td>TTPs</td>
<td>tactics, techniques and procedures</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications Service (3G)</td>
</tr>
<tr>
<td>UPS</td>
<td>uninterruptible power supply</td>
</tr>
<tr>
<td>US NCSC</td>
<td>United States National Counterintelligence and Security Center</td>
</tr>
<tr>
<td>VOIP</td>
<td>voice over internet protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>WA</td>
<td>Wassenaar Arrangement</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
<tr>
<td>WAP</td>
<td>wireless access point</td>
</tr>
<tr>
<td>WEP</td>
<td>wired equivalent privacy</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>wireless fidelity</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi protected access</td>
</tr>
</tbody>
</table>
Data and information have been important for a very wide variety of reasons and for as many centuries as man has been able to pass valuable data to another person. The location of the nearest water hole, herd of wild animals or warm cave was a carefully guarded secret that was only passed on to those with a need to know and who could be trusted not to divulge the information to other, possibly hostile, tribes. The methods of transfer and the storage of such information were perhaps rather more primitive than today, but the basic principles of information security have not changed too much since those days.

Information assurance is now well founded in three major concepts – those of confidentiality, integrity and availability. Managing these concepts is critical and, as information has increasingly become one of the modern currencies of society, it is the retention of assurance in an appropriate and cost-effective manner that has become of keen interest to businesses in all sectors, of all sizes and in all locations. Specific measures taken to ensure that information is held securely is termed ‘information security’ – the way of achieving information assurance.

As an example, even within living memory, the quantity of numbers we are given and need to enable us to exist and participate in modern society has risen almost exponentially from virtually zero in the early part of the 20th century, to several hundred (and still growing) now: PIN codes; licence numbers; credit card numbers; number plates; telephone numbers; employee number; health, tax and insurance numbers; access codes; customer numbers; train times; tram or bus numbers; and so on. We now need to remember such numbers on a day-to-day basis, and that is before we start work proper and have to deal with all those things that allow us to earn our salary, where even more numbers and other elements of information will occur.

The mechanisms we use to manage information are the areas where we have seen very significant change, notably in the last few decades. The advent of computers in particular has extensively altered the way we manage information and has also meant that we have much more information to worry about than ever before. Information has become the key to success in almost any field and so the assurance of it has gained in significance and, perhaps more importantly, in value to a business or organisation. It may not necessarily be financial value that is the most important factor. Lack of knowledge of some issue or the way things are done, or knowing the currency of specific pieces of information may be more important than any financial valuation. Nevertheless, looking after it properly is still very important.
One other factor that has significantly altered our need for assurance of information is that of mobility. Life was straightforward when the only place we had business information, and where we were able to look after it properly, was the office – to secure information, we closed and locked the office door. Today we expect and need to have information in a wide variety of locations, including wanting it on the move in cars, trains and planes. With open plan offices and the increasing mobility of the office environment, we now have a critical need for improved assurance if we don’t want others to gain access to our information inappropriately.

Threats, vulnerabilities and countermeasures have also changed and grown in complexity in some areas, although it is still essential to consider the easiest and often cheapest countermeasures before getting into large or expensive solutions. The increase in capability of those intent on causing harm to companies, public bodies and other organisations means that the role of the information assurance manager and the professional has increased in complexity to such a degree that it is now quite possible to have a full and very satisfying working life entirely within this field of expertise.

Since the late 1980s a new term that has come to prominence is ‘cyber security’. The reasons for this are largely down to the significant increase in threats – the complexity of threats, the number of threats and the potential impact of threats – that now arise from the internet and the use of the World Wide Web. Cyber has been used to describe the risks and vulnerabilities that arise primarily from the use of the internet and so cyber security has become the most commonly used term to address these areas. In this edition of this book, we have continued to use the term ‘information assurance’ where general principles are discussed, have used ‘information security’ again where it is the most appropriate term, but have also referred to ‘cyber security’ where the threats are specifically internet based. With the seemingly meteoric rise in what are now known as cyber-attacks, we see more and more attempts to misappropriate information. Criminals and others want to steal information and sell it on or use it for other purposes; to encrypt information and then demand money to release it back to its rightful owner; and to use information gained fraudulently through any means to extract financial gain from seemingly innocent victims, be they businesses or individuals. This is cyber warfare and leads to cyber security.

The legislation that is introduced by governments to address the increasing problems of information assurance in all its guises, is also an area of concern and this book covers the most important principles and the implementation of such laws. Once again, though, it is important that you understand that this book has been written in the UK and is based on English law. Other countries, even Devolved Administrations within the UK, may have further or different legislation with which you should become acquainted. Reference has been made to national and international standards applicable to information assurance, but there is no requirement in the examination for the BCS Certificate in Information Security Management Principles (CISMP), upon which this book is based, for detailed specific knowledge of any of those standards. They are naturally important, but it is recognised that they will change over time and be more applicable in some parts of the world than in others. You should ensure you are familiar with the standards relevant to your country, your area of interest, your organisation and your business sector.

This book accompanies the BCS Certificate in Information Security Management Principles. This qualification, one of a series covering the whole area of information
assurance management, is the first step towards a full understanding of the issues and the comprehensive management of the assurance of information wherever it may be. This book is intended to be a first read for those new to information security and concentrates on the high-level principles. It is not intended to be a comprehensive guide to everything that a practitioner in the area would need to know.

The technical aspects of information security, including the technical details of information systems (IS), computer networks, communication systems, cryptography and related areas, are not part of the syllabus for this qualification despite their importance. However, they appear in higher qualifications, so in this book reference is made to them in passing but they are not covered in any detail. The syllabus and this book have remained technology neutral as far as possible.

While BCS, The Chartered Institute for IT, is clearly mainly concerned with the impact and effective use of computers, it is recognised that it is impossible to divorce the management of information security in computers from the management of information in any other media or from the security of the tools used to process information. Thus, in this book, the boundaries between different forms of information storage, processing, transmission and use are deliberately blurred or indeed removed entirely. It is not significant whether a particular piece of information exists in electronic form, paper form or indeed in someone’s head. Its appropriate protection is the main factor, and all aspects of its assurance must be considered from all angles.

The latest version of the examination syllabus can be downloaded from the BCS website and it is the guide for the contents of this edition of this book. As a result of studying this book, you should gain a very clear understanding of the various elements of information assurance and should be able to consider taking the professional examination. It would naturally be useful for an individual to undertake a period of study with an approved training provider to enhance their understanding, and those who deliver such training will inevitably add value to the knowledge given here, probably increasing the chances of success in the examination.

There are some areas where this book does not provide all the detail necessary to answer all the questions in the examination, but there are ample suggestions for additional study and resources for further reading that would help. A simple scenario has been introduced in order to help develop full understanding and to provide a close-to-life example of the real world. Activities based on the scenario are suggested throughout the book, again to help bring reality into the concepts discussed, and it is hoped that you will do these in an appropriate manner – formally or informally as suits you best. The format of the multi-choice questions in the book is broadly in line with the questions in the examination, but naturally there will be different questions in that. A sample examination paper can also be downloaded from the BCS website.

After studying this book and the related syllabus, you should be able to demonstrate a good knowledge and basic understanding of the wide range of subject areas that make up information assurance management. The examination tests the knowledge of principles rather than the knowledge of specific technologies, products or techniques. This means that where in the book specific technical examples are used to illustrate particular principles, it is the understanding of the principles that is of prime importance when considering the examples, and not the examples themselves. If more information is required in specific areas, such as risk management, business continuity or project management, other BCS publications are available that provide a much deeper understanding. Full details of appropriate publications can be found on the BCS bookshop.²
1 INFORMATION SECURITY PRINCIPLES

This chapter covers the basic principles of information assurance (IA). It introduces some specific terminology together with its meaning and definitions and considers the use of such terminology across the field of information assurance management. It also discusses the way in which information assurance management relates to its environment.

CONCEPTS AND DEFINITIONS

As in any area of business, information assurance management has its own language, although, being very closely related to business need, it is limited in scope and complexity to enable the wider business population to appreciate the concepts with little difficulty. Each of the terms listed below will be further discussed and expanded upon later in the book in the appropriate section.

In the following sections the definitions in italics have been taken from the BS ISO/IEC 27000 series of standards (latest editions at the time of writing) where the definition exists, and from other ISO standards where there was no 27000 definition. Where there is no extant definition, it is provided by the authors or from other sources, noting its source where applicable.

LEARNING OUTCOMES

Following study in this area, you should be able to define and explain each of the following terms and to describe their appropriate use as applicable.

Information security

Confidentiality. The property that information is not made available or disclosed to unauthorised individuals, entities or processes (ISO/IEC 27000)

Information will often be applicable only to a limited number of individuals because of its nature, its content or because its wider distribution will result in undesired effects, including legal or financial penalties or embarrassment to one party or another. Restricting access to information to those who have a ‘need to know’ is good practice.
and is based on the principle of confidentiality. Controls to ensure confidentiality form a major part of the wider aspects of information assurance management.

**Integrity. The property of accuracy and completeness (ISO/IEC 27000)**

Information is only useful if it is complete and accurate, and remains so. Maintaining this aspect of information (its integrity) is often critical and ensuring that only certain people have the appropriate authority to alter, update or delete information is another basic principle of IA.

**Availability. The property of being accessible and usable upon demand by an authorised entity (ISO/IEC 27000)**

Information that is not available when and as required is not information at all but irrelevant data. Availability is one area where developments in technology have increased the difficulties for the information assurance professional very significantly. In the past, in an ideal world, all important information could be locked up in a very secure safe of some form and never allowed to be accessed – just about perfect assurance but, naturally, totally impractical. There will, therefore, always have to be a compromise between security in its purest sense and the availability of the information. This compromise has to be acknowledged throughout all aspects of IA and has a direct bearing on many of the principles covered in this book.

**DATA OR INFORMATION?**

Data (sometimes clarified as raw or unprocessed data) are generally accepted as being the basic facts and statistics that can be analysed and subsequently used for many different purposes.

Information is the result of the analysis of the data – the refined information that is useful to operators and managers to understand what is going on; for example, on their IT systems.

**Assets and asset types**

**Asset. Anything that has value to the organisation (ISO/IEC 13335)**

Assets come in as great an array of types as the mechanisms for using them. In information assurance, three main types of assets are considered, although the sub-categories that fall within each of these main types can be numerous. The three main types are:

1. pure information (in whatever format);
2. physical assets such as buildings and computer systems;
3. software used to process or otherwise manage information.
When assets are considered in any aspect of IA, the impact on all three of these asset types should be reviewed. The value of an asset is usually estimated on the basis of the cost or value of its loss or unavailability to the business through a business impact assessment. There are, however, other aspects to consider, including, but not limited to, the value to a competitor, the cost of recovery or reconstruction, the damage to other operations and even the impact on such intangibles as reputation, brand awareness and customer loyalty.

**Threat, vulnerability, risk and impact**

The understanding of these terms is critical to the whole of information assurance.

*Threat.* A potential cause of an unwanted incident, which may result in harm to a system or organisation (ISO/IEC 27000)

A threat is something that may happen that might cause some unwanted consequence. As a simple example, if we see clouds in the sky that look large and dark, we talk about the threat of rain. Naturally, to some this threat is not unwanted at all, farmers perhaps, and so they would not have the same view of the clouds and their potential for rain – and this is an important point to recognise. Threats to one organisation may well be opportunities to another, it is all very dependent on the viewpoint, the environment and the situation in which they are being considered.

*Vulnerability.* A weakness of an asset or control that can be exploited by one or more threats (ISO/IEC 27000)

A vulnerability is a weakness; something that, if exploited, could cause some unwanted effect(s). To continue the example above, if someone was to venture out into the cloudy environment without an umbrella, this could be considered a vulnerability. If something (the threat) happens (it rains) then the consequences could be detrimental.

*Risk.* The effect of uncertainty on objectives (ISO/IEC 27000)

Risk, then, is the combination of these two. If there is a threat (of rain) and a vulnerability (of not carrying an umbrella) then there is a risk that the individual concerned might get wet and ruin their expensive clothes. There may well be other risks associated with this same set of circumstances – ruined hair style, late attendance for an appointment, and so on. It is also important to recognise that sometimes there may be a combination of circumstances that lead to further, more serious risks as well. The lateness of attendance at an appointment combined with a number of other similar occurrences could result in termination of employment. It should be noted, however, that if either the threat or the vulnerability is removed in some way, there is no longer a risk. Both must be present for the risk to exist at all.

*Impact.* The result of an information security incident, caused by a threat, which affects assets (ISO/IEC 13335)

The impact of the risk actually occurring is perhaps the most important concept of all to grasp. It is the potential impact that has to be considered and managed in IA. If the impact is small and insignificant – a wet coat in the example above – then it may be
entirely appropriate to accept the risk and to take no further action other than to monitor it. On the other hand, if the potential impact could be dismissal from a well-paid job, then more appropriate countermeasures need to be considered – the purchase of an umbrella, hiring a taxi or similar. As far as businesses are concerned, the impact on the organisation and its daily activities is usually the crucial consideration and will often warrant further measures being taken.

Information security policy concepts

Any organisation should have a policy for its management of IA. This is normally a short, punchy statement from the chief executive stating that they acknowledge the risks to the business resulting from poor information assurance and will take appropriate measures to deal with them. It should include statements that make it clear that the organisation regards risk as a serious issue, with it being discussed at all appropriate meetings, with those with the correct authority and responsibility taking an active interest in it. It is common for organisations to form an information assurance or security working group to lead the activities necessary to ensure appropriate levels of assurance within the organisation.

The purpose of controls

Controls in the IA sense are those activities that are taken to manage the risks identified. There are four main types of strategic control, although the actual implementation of each of these types can be very varied.

Eliminate. Risk avoidance – Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk (ISO Guide 73)

This means taking a course of action(s) that removes the threat of a certain risk occurring at all. This could entail removing a particular item that is unsafe, choosing to do things in a completely different way or any number of other options. This action is sometimes referred to as ‘prevent’, ‘avoid’ or ‘terminate’.

Reduce. Risk reduction – Action taken to lessen the probability, negative consequences, or both, associated with risk (ISO 22300:2018)

This means to take one or more actions that will reduce the impact or the likelihood of a risk occurring. It is rare for an action to both reduce the likelihood and reduce the impact of a risk. It is often necessary to use several of these measures in partnership to have the desired overall effect. This could include having contingency measures in place that mitigate the effect if the risk does occur – a backup plan or ‘plan B’. This action is sometimes referred to as ‘treat’ or ‘mitigate’.

Transfer. Risk transfer – A form of risk treatment involving the agreed distribution of risk with other parties (ISO Guide 73)

This means to take steps to move the accountability for a risk to another organisation who will take on the responsibility for the future management of the risk. In practice, this might mean taking out some form of indemnity or insurance against the risk occurring or perhaps writing contracts in such a way that the financial impact of a risk
occurring is borne by a third party – liquidated damages. It should be noted though that, for example, taking out an insurance policy to cover the costs of rectifying the results of a risk happening will often not take away the impact. Reputation is the most common example where, although the insurance company may pay out the costs incurred by the client in dealing with an issue, the reputational damage to the organisation may still be very evident. This action is sometimes referred to as ‘share’.

**Accept. Risk acceptance – The decision to accept a risk (ISO Guide 73)**

This means senior management accepting that it is not considered practical or sensible to take any further action other than to monitor the risk. There could be a number of reasons why further actions are considered inappropriate, including but not limited to: the likely impact of a risk is too small; the likelihood of a risk occurring is too small; the cost of appropriate measures is too high in comparison with the financial impact of the risk occurring; the risk is outside the organisation’s direct control. The decision is also related to the organisation’s risk appetite, which determines the level of risk the organisation is prepared to accept. This is sometimes referred to as ‘tolerate’ but should not be termed the ‘do nothing’ option.

**Identity, authentication and authorisation**

*Identity. Information that unambiguously distinguishes one entity from another one in a given domain (ISO/IEC 24760-1)*

Frequently there is a need to establish who is accessing information, and the identity of individuals may well be required. This may enable, for example, audit trails to be produced to see who changed a specific item of data and hence to assign an appropriate level of confidence to the change. This concept is equally applicable to assets such as specific pieces of information that need to be identified uniquely.

*Authentication. The provision of assurance of the claimed identity of an entity (ISO/IEC 15944-6)*

This process ensures that the individual is who they say they are and confirms their identity to an appropriate level of confidence appropriate for the task in hand. This could be simply asking them for their date of birth, at the most basic level, through to completing a complex identity check using, for example, tokens, biometrics and detailed biographical-data checks.

*Authorisation. The right or permission that is granted to a system entity to access a system resource (ISO/TR 22100-4)*

In order for anyone to use a system of information retrieval, management and so on, it is good practice to have a method of authorisation that makes clear the assets to which someone should have access and the type of access they should have. This authorisation will vary depending on the business requirement, the individual, the type of asset and a range of other aspects. Who has the authority to detail and approve such authorisations will vary according to the type of usage required.
Accountability, audit and compliance

Accountability. The property that ensures that the actions of an entity can be traced uniquely to the entity (ISO/IEC 21827)

When any action is carried out on an information system or as part of the information assurance management system, an individual needs to be accountable for that action. The person who has the accountability may delegate the actual work to someone else, but they still retain the accountability.

Audit. The review of a party’s capacity to meet, or continue to meet, the initial and ongoing approval agreements as a service provider (ISO 15638-15)

This is the checking (formal or informal) of the records of a system to ensure that the activities that were anticipated to have taken place have actually happened. The purposes of an audit could include identifying gaps in the system’s functionality, noting trends over time to help with problem resolution or identification, or a number of other requirements. It can also help to identify misuse of information or the inappropriate use of an authorisation, for example, and thus identify unauthorised activity.

Compliance. Meeting or exceeding all applicable requirements of a standard or other published set of requirements (ISO/TR 19591)

Ensuring that a system or process complies with the defined or expected operating procedure is compliance. This could cover a major operation, such as a whole organisation being compliant with a recognised national standard for information assurance, or could be much more limited with just certain aspects of the operation, or even individual users of a specific system being compliant. In general, compliance should be independently audited to achieve certification against a standard; for example, a legal or regulatory framework.

Information security professionalism and ethics

General awareness of the work done by information assurance professionals (as distinct from IT security professionals) is gradually growing as organisations become increasingly complex with more and more information being managed and processed. The adage that the staff are the most important asset of an organisation could now be seen to be outmoded since it is often the case that it is the information an organisation holds and uses effectively that has become its most important asset. Therefore, looking after it has also increased in importance and the whole profession has grown to meet the need. Professional bodies, such as the Chartered Institute of Information Security (CIISec) (previously the Institute of Information Security Professionals (IIISP) that was set up in 2006 in the UK), have helped to raise the profile very significantly, as have the various qualifications ranging from this introductory level to Masters degrees and beyond.

The UK’s National Cyber Security Centre (NCSC) have developed a certification scheme (the Certified Cyber Professional (CCP)) where individuals can demonstrate their competence and experience to independent assessors from a certification body, who
will recommend the award of a certificate in a specialism when the appropriate criteria have been met.

An information assurance professional will, inevitably, become party to some of the most important information an organisation might hold. This could be sensitive for a number of reasons, but in all cases it is critical that the professional deals with it in the appropriate manner. Releasing information to a third party or other organisation, albeit with the best of intentions but without the approval of the owner, is probably one of the easiest ways to be dismissed. Non-disclosure agreements (NDAs) are now commonplace even in seemingly innocuous areas such as publishing and the retail marketplace, as well as the more usual research and development, product innovation and financial areas.

The bottom line of all assurance is trust. Without it, it is impossible to operate in the world as it is today. The degree of trust is where there is room for manoeuvre and it is often the degree to which staff, customers, suppliers, shareholders and the like can be trusted that will determine the measures that have to be put in place. It is crucial though that the trust placed in information assurance professionals is not misplaced in any way. They must be above reproach and never be seen to compromise in this critical area.

**The information security management system concepts**

*Information Security Management System (ISMS). Part of the overall management system, based on a business risk approach, used to establish, implement, operate, monitor, review, maintain and improve information security (ISO 12812-2)*

The main principle behind the ISMS is that there should be a ‘one-stop shop’ for all information pertinent to the assurance of information within an organisation. As soon as there is a need to go looking for documentation, policies, practices or anything else to do with assurance, the chances are that someone will not bother and will do their own thing.

While there may well be good reason for them not to do this in terms of rules, regulations, punishments and the like, human nature being what it is, they will find a reasonable excuse for going down a different route if only because ‘I thought it was OK and couldn’t be bothered to check if it was the right way to do it.’ The result of this approach will inevitably be a reduction in the overall level of assurance. In addition, any system that is too complex or difficult to use will result in users finding ways to get around the security measures put in place, perhaps again resulting in weakened assurance.

It is critical, therefore, that organisations make their information as freely and easily available as is possible, practical and necessary and this equally applies to the security rules controlling it. Naturally there will be elements of policy that have to be more secure, available only to those with a strict need to know, but in general everyone should be able to access easily and quickly the appropriate information and the security measures pertinent to it.
Information Security Management Principles

National and international security standards

As a policy, BCS have decided not to relate the syllabus for the BCS Certificate in Information Security Management Principles to any national or international standards or frameworks for information security specifically, although there are many such documents that are applicable. The main reasons for this were two-fold: first, to make the syllabus and the qualification as applicable internationally as possible and, second, to reduce the need to update the syllabus at every change to the standards.

It is clear, however, that IA is the subject of several international and national standards and that these should be considered when studying for the examination. The questions set in the examination will never be specific to any one standard, but will be generic to all best practice where applicable. The knowledge of the appropriate standards required for the examination is therefore limited to a general understanding of the principles involved as they reflect on best practice. In the UK, awareness of, for example, the ISO/IEC 27000 series and related British standards is helpful but not critical to the passing of the examination. It is the broad principles that should be used as a basis for study, as reflected in the examination syllabus.

There is, though, another aspect of this. When an information assurance professional is working in an organisation to deliver a secure and effective information management system, the relevant standards should always be viewed as the achievable goal for the system. Whether it is necessary to gain simple compliance or go the extra step to achieve certification is an arbitrary decision often based on other factors. Nevertheless, it is considered good practice to base an effective information assurance management system on the principles of the relevant standards. The use of an internationally accepted standard such as the ISO/IEC 27000 series makes sense in the global nature of operations today.

The Group for the Appreciation of the Natterjack Toad Scenario

The Group for the Appreciation of the Natterjack Toad (GANT) is a conservation group that is keen to promote and preserve the well-being of the Natterjack toad. It has a significant number of members in many different countries around the world, all of whom are keen to promote the work of the Group, which is a charity registered in the UK. All of GANT’s information is either on a web-based application available to members over the internet or on old-fashioned, paper-based documents held by Dr Jane Peabody, the honorary secretary/treasurer.

The Natterjack toad is an endangered species that is gradually being destroyed by the development of areas where it prospers and through pollution affecting the brackish water and sand dunes in which it lives.

The membership of the organisation is growing and the system for managing the records of members is one area where there are some concerns about information assurance. Details of GANT’s activities, their meeting places, their website and
other aspects of the Group’s work have been compromised in the recent past owing to the server containing them having no significant security in place. The chairperson (Ms Rachel Jackson) believes it is the right time to take information security more seriously. She has heard a bit about information assurance but needs to be clear what it really means and, most importantly, what the benefits and costs would be to the organisation.

The GANT scenario in the box above is a fictitious scenario that will be used throughout the book to provide examples and to be the basis of some questions to aid your understanding of the theory. The main objective of the scenario is to implement an effective IA system, but we will take you through various steps along the way to help with your understanding.

ACTIVITY 1.1

Assume that you have been invited to a committee meeting of GANT by the chairperson, who wants you to 'start the ball rolling' by explaining why it would be a good idea for GANT to think about information assurance.

To make your points most forcefully, she has asked you to define three threats to the organisation, three vulnerabilities and consequently three risks that any information assurance system would need to manage.

We have started above with developing an initial idea of the reasons for considering IA based on three possible problems. We will take that on to a more formal approach in due course – this is simply to get you thinking about some of the terms we have introduced in the first section of the book. Solution pointers for all the activities are at the end of the book.

THE NEED FOR, AND BENEFITS OF, INFORMATION SECURITY

Any business will have information that is critical to its continued effective operation. Looking after this information in an appropriate way does not come free but has a price tag attached that can be, in some circumstances, very considerable. It is therefore essential that information assurance professionals are able to justify their recommendations for appropriate security measures in a sensible yet pragmatic manner, which must take into account the specific environment in which the business is based.
LEARNING OUTCOMES

Following study in this area, you should be able to explain and justify each of the following concepts and to describe their appropriate use as applicable.

The importance of information security as part of a business model

Information security – Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO 19092)

Neither information nor assurance operate in a vacuum. Both need to take into account the environment in which they are operating and address the issues that this environment brings with it. It is therefore critical that any information assurance system must be grounded firmly in the business world. This means that IA is not an issue only for the IT manager or the security officer but for the whole organisation. As soon as only one part of the organisation is given the task of running assurance, the rest of the organisation will bother less about it. All staff members of any organisation, regardless of its nature, its business, its location or any other factor, should be concerned about IA. It might be from a purely personal viewpoint (what happens to my personal data in this place?) or from a wider view of the effective, continued operation of the organisation, but in either case everyone should be concerned and involved.

Information assurance (IA) – The confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users. (UK Cabinet Office)

Physical, technical and administrative controls are needed to accomplish these tasks. While focused predominantly on information in digital form, the full range of IA encompasses not only digital but also analogue or physical form. These protections apply to data in transit, both physical and electronic forms, as well as data at rest in various types of physical and electronic storage facilities. Information systems include any means of storing, processing or disseminating information including IT systems, media and paper-based systems.

Assurance should not be viewed as an ‘add-on’ to be included only if there is the time and the money to do it. It has to be built-in to business processes at all stages if it is to be truly effective. While it might be possible in some areas to add in security measures at the last moment (an extra lock on a door or an additional staff security check, for example), they will usually cost more and be less effective than if they had been added at the appropriate time earlier in the design process.

Different business models and their impact on security

In the last 20 years, the world of business has changed dramatically – perhaps more than in the previous 50 or 100 years. One of the principal reasons for this is the increased use of technology that has enabled business to be transacted remotely rather than in person. One of the consequences of this is that more people are able to make business
transactions themselves rather than expecting others to act as intermediaries. No longer do we need to use travel agents to book our flights, local garages to obtain our cars for us or financial advisors to obtain investment packages for us. All these and many more transactions can be carried out directly with the supplier, often using the internet for communications, or with a trader in another part of the country or the world who can offer a better deal. While the access to such facilities is a huge advantage and can provide very significant financial savings, among other benefits, it has brought with it major issues of security both for the individual and for the organisation wishing to trade in this way.

The other very significant change in business has been the shift in the UK away from manufacturing and related primary industries to service and financial industries where the use of technology has an even bigger impact.

It is clear that the use of technology in manufacturing has changed those industries too but, it might be argued, in a more controlled and manageable manner. However, it would be wrong to assume all is well in the factories; issues with the security of industrial control systems (ICSs) are increasing in number and severity. There will be more about this specific issue later.

In the service industry, the availability of information has increased many times over and has liberated the industry in a manner that is similar to the impact of the introduction of the steam engine or electricity in their day. This in turn has increased the importance and difficulty of keeping the information secure.

Many organisations are now based and/or operate in more than one country. With global organisations now moving very sensitive information or other assets around the world at a moment’s notice, the need to ensure it is done securely and with proof of receipt, integrity and authority has grown too. Proving that the authorised person sent the correct document at the appropriate time only to the intended recipients, not to mention ensuring that it arrives in the same state as when it left the originator, are all issues that the information assurance manager now has to deal with to the satisfaction of their management and any ambitious litigant. In addition, organisations that operate within different countries need to understand the differing restrictions that local legislation may place on how their information can/must be handled.

There are many further risks from this change in business model. With an increasing amount of trade being conducted across the internet, organisations must be aware of the dangers of virus infection including ransomware, denial-of-service attacks, unauthorised changes to their information in the public domain (e.g. websites) and the impact of any such issues on their reputation, financial status and other related areas. In addition, organisations are having to deal with people about whom they know very little but with whom they still need to establish an appropriate level of trust. The ability of disillusioned employees, ex-employees or groups of activists to damage an organisation by taking, deleting, altering or otherwise misappropriating critical business information from the employer, and either passing it to a competitor or simply using it for their own ill-gotten gains, is now a very real issue. Companies who have been the victims of such events are not inclined to increase the damage caused by making such acts public knowledge if they can avoid it; however, there are many apocryphal tales of the theft of client databases, deletion or alteration of critical financial data and other similar acts, which suggests that some at least are true.
There are also cautionary tales of laptop PCs containing highly sensitive or confidential information being lost or stolen from parked cars, to the embarrassment of the company or organisation. All mobile devices, such as tablets, smartphones and the like, are seen as easy targets for the attackers and, since many such devices are under the ownership of an individual rather than the organisation whose information may be accessed or held on it (what is usually labelled as bring your own device, or BYOD), the way this attack vector is managed has to be considered very seriously.

The use of the internet for transactions, be it shopping for cars, food or financial services, as well as the storage of client, stock, financial and related information in a secure manner, has further increased the problems to be managed. Often this storage is no longer in a place accessible by the owner of the information, since it is stored in a cloud-based system potentially anywhere in the world. This has given rise to the term ‘defence in breadth’, which means that all connected systems must now be taken into account when considering how an attack might materialise and the effect it might have. The systems of suppliers and advisors may well be an easier way into the more secure systems of an organisation, since the supplier is a trusted partner and perhaps not subject to the same level of security scrutiny as someone coming in from the outside. This aspect is countered by using defence in depth: layers of security that may start off as relatively low level, but which can increase in complexity, cost and effectiveness as the information and systems being protected get more and more sensitive or important. It should not be a straightforward activity for a criminal to gain access to a low value system or network and to be able to traverse into more complex and sensitive areas without significant additional security measures being encountered.

The ability of the consumer to deal directly with the manufacturer has increased the risks for industry as well as for the consumer, as the problems of unreliable services or products still abound. With the rise of business-to-business transactions, just-in-time operations and other similar services that rely heavily on the timely and accurate movement, storage and retrieval of critical information, the loss of a computer system for a comparatively short while can and has created serious financial losses for the businesses concerned.

The UK’s Department for Digital, Culture, Media and Sports (DCMS) estimated in their Cyber Security Breaches Survey 2019 that there was an average cost of a single cyber-attack on larger businesses (those with more than 250 employees) of around £22,700, in direct costs. This figure does not represent the whole story, as indirect costs such as reputational damage and loss of productivity were not really included. The incidence of cyber-attacks has also continued to increase according to the survey, with 61 per cent of large businesses reporting a cyber-attack in the previous 12 months.

The effect of the rapidly changing business environment

‘It is change, continuing change, inevitable change, that is the dominant factor in society today.’ This quotation is from Isaac Asimov, and it is now well understood that for a

business to survive in the current climate of change, it must adapt and be able to adapt rapidly. This means that what was acceptable as a business practice last week may no longer be acceptable this week; therefore, any assurance system put in place must reflect this changing climate and be flexible enough to cope with it. However, this does not mean that the assurance can be relaxed or reduced in any way. Indeed, if anything, the flexibility should produce a higher level of security and assurance that risks are being managed effectively.

**Balancing cost and impact of security with the reduction in risk**

Life can never be risk free. In fact, it is often considered that life is all about risk and its effective management. The measures taken in an organisation to reduce risk to an acceptable level can at times become excessively expensive. A careful balance must be struck between the cost or business impact of a risk if it occurs and the cost of the measures taken to reduce its likelihood or impact.

A typical example is insurance. An insurance policy may help to offset the cost of a risk occurring by providing the necessary financial backing to be used to deal with the occurrence of a risk. However, if the cost of the insurance policy is too high, it may simply be cheaper to accept that the risk might occur and pay the smaller amount out to deal with its consequences. It must also be remembered that while it may be possible to transfer to a third party some of the impact of a risk occurring – the financial impact, for example – it is frequently very difficult to transfer the other consequences of a risk, notably the impact on reputation, public opinion or other related results.

It is not uncommon for organisations to put in place extravagant measures to reduce the impact or likelihood of risk occurring when in reality the consequences of the risk occurring are limited, or the actual chance of it happening is so small that the expense is a waste of both money and effort in managing the risk unnecessarily.

A second problem is that of maintaining the currency of risk countermeasures. Once defined and planned, it is critical that they are not simply put on the shelf to await the risk arising. The world around us changes and so the countermeasures may not be valid or may change in their effectiveness or cost as time moves on. Thus, risk management, and the maintenance of the consequential actions taken, is a continual and iterative process that must not be allowed to whither through lack of action or misplaced belief that the situation will not change.

**Information security as part of company policy**

Assurance or security is not an add-on. It is not possible to deal adequately with assurance by considering it as an additional expense to be avoided if at all possible. The most effective way to deal with it is to include it from the beginning in all areas of the organisation. To this end, the inclusion of assurance as part of the operational policy of the organisation is the only cost-effective way of covering the issues adequately.
There are clear similarities between information assurance and health and safety issues. As soon as health and safety are seen as one person’s problem (that of the health and safety officer), the battle for a safe working environment has been lost. Similarly, assurance is not the concern solely of the information security manager, but of the whole organisation. It is essential also that this involvement is from the top of the organisation to the bottom. Just implementing IA at middle management or on the shop floor is meaningless and will inevitably lead to further assurance issues. Senior management have a critical role to play to ensure they engender a working environment where IA is the norm and accepted by all.

The need for comprehensive policy, standards, guidelines and procedures documentation

Just having a policy for information assurance or information security on its own is meaningless. It must be fully supported by a range of other documentation covering the standards expected, the guidelines of how to do things correctly and procedures for what must be done to preserve the assurance of the information in question. This documentation must be comprehensive but digestible, pithy, something that can be read easily and something they will actually read. Not a 1,000 page document that, with all good intentions, the average Joe will not read.

It is good practice to ensure that any procedures to be followed are detailed in an easily digestible format, perhaps as desk cards or prompts for users, or as checklists for operators or support technicians. It must be remembered, however, that this is not only about computers. For example, procedures are also required for the management of physical assets such as filing cabinets, including how they should be cleared before their disposal to avoid the inadvertent inclusion of a confidential file for the second-hand filing cabinet marketplace. Where information critical to the organisation’s continued operation is held solely in the heads of its staff, it is almost inevitable that one day this will result in one of the key staff members being ill, having an accident or being otherwise indisposed when a crucial decision or operation is required. Considering the management of the information in staff members’ heads is just as important as the effective management of technical systems – some might say more so.

Relationship with corporate governance and related areas of risk management

In recent years the advent of some very-high-profile commercial criminal investigations have resulted in much more stringent and invasive legislation regarding risk taking in companies. Sarbanes–Oxley from the USA, the effects on corporate governance of the Turnbull Report, the Companies Act in the UK and related issues have all had the effect of bringing risk management to the top of the agenda in many boardrooms. It is no longer effective or acceptable (if it ever was) to delegate the responsibility for risk management down to the manager of the IT section.
The proper implementation of effective IA should lie at the heart of all organisations regardless of their sector, size or business. Properly implemented, the secure management of information can provide assurance that risk is being managed effectively in that area at least and can form the firm foundation for further risk management in related areas. If all information is covered by the measures implemented, then the financial, operational, intellectual property rights and a whole range of other risk areas can be managed through the establishment of a single framework.

**Information and data life cycles**

Information and data have a similar life cycle, and this will be discussed in more detail in Chapter 4.

**Security as an enabler delivering value rather than cost**

In the information economy in which we all now live, the cost of the loss, corruption, non-availability or unauthorised release of information can be very high. The effective implementation of IA measures can have a very beneficial effect on the potential costs of such events. Thus, it is easy to develop a convincing and compelling business case for the effective management of information through the use of an approved standard and related processes. While it may not be possible to remove the risk entirely, it should be possible to ensure at least that the probability of the risk occurring is significantly reduced or that the effects of the risk materialising are significantly reduced in terms of the business impact.

The use of appropriate countermeasures and contingency plans can also have the very beneficial effect of making the work done by an organisation much more orderly by being based on best working practices. Piles of paper and computer disks left lying around on desks, floors and shelves can be a security disaster waiting to happen. With an IA standard in place, such things should be a thing of the past and the need to spend many hours finding a specific piece of information should be long gone.

With the advent of photocopiers in almost every workplace, the ease with which a sheet of information could be reproduced became very much greater. This in turn meant that where initially there might be only the original and perhaps one handwritten copy of a document to look after, there was now the possibility of many copies to worry about and to try and control. Many a leak from organisations, including governments, has been caused by the proliferation of photocopies, mislaid CDs or inappropriate, perhaps covert, use of USB memory sticks. With improved working practices instigated through effective IA, the need to reproduce information declines, since those who need to see a piece of information can do so easily and in a controlled way through the appropriate use of technology, perhaps without recourse to the production of ever more duplication.

---

3 An example of which is shown in the film *The Post* (2017) – the true story of how journalists from the Washington Post newspaper exposed the American government’s ongoing involvement in the Vietnam war, using photocopies of Pentagon papers.
The role of information security in countering hi-tech and other crime

Crime is always advancing and developing, often a little quicker than the enforcement agencies who are established to combat it. The hi-tech industry (covering computers, the internet, digitisation, communications and related areas) over the last 30 years or more has provided criminals with ever-increasing opportunities for more advanced and profitable crime in a wide range of activities. Some crimes are old ones, which have effectively been removed from the criminals’ handbook. One example is that of fraud, which had been dealt a severe blow by the introduction of sophisticated security devices in banknotes, passports and the like, but, with the ever-increasing use of the internet, has now returned with increased ‘effectiveness’. Emails with ‘too good to be true’ headings, such as lottery win notifications, have been estimated to be responsible for an overall loss well into the millions of pounds in England and Wales alone. What is commonly referred to as invoice fraud, when a company or organisation is tricked into changing bank account payee details for a sizeable payment, is becoming increasingly common, with ever-increasing sums of money being taken.

Instances such as these are no more than old-fashioned fraud dressed up in new clothes. In addition, the ability to obtain personal information through phishing, key-loggers, screen-scraping or similar tactics has increased the opportunities for criminals to achieve their nefarious purposes. Social engineering helps too; for example, in persuading perhaps more junior members of staff to undertake inappropriate financial activity in a company by apparent pressuring from a supposed senior colleague. Often, simple procedural steps could help to reduce the risk of these crimes – techniques totally separate from the electronic mechanisms through which the crime is committed.

IA can help to address all these issues, at least in the workplace. Good practices at work can also lead to better practices at home, where the proliferation of computers in particular has led to increasing instances of criminal activity targeting the home user. The social duty of companies to help reduce crime overall is well established and setting good work practices with the care of information is an excellent opportunity that should not be missed.

The growth of such crime has increased the importance of forensic investigation, and notably the requirement to preserve evidence based on IT systems. Later in this book this subject will be discussed in more detail, but in recent years it has been ever more evident that the skill of the IT practitioner in the preparation of evidence for trials has needed to develop very considerably from the early days of computing, when IT evidence was rarely used except in the most complex of cases. Now, with internet-crime on the increase and the use of IT becoming the norm for many areas of criminality, the use of investigative techniques based on IT systems has increased enormously. With effectively managed IA high on the priority list for all organisations, these techniques are now a vital piece of the jigsaw of helping to reduce criminality. The IA professional is now a crucial element in the fight against crime, both internal and external to the organisation itself.

---

4 Crime in England and Wales: year ending March 2019 (ONS.gov.uk).
Ms Jackson, the chairperson of GANT, has asked you to help to develop a sound business case for the implementation of an ISMS. She needs to be able to convince her fellow committee members to authorise the expenditure and so needs to be clear about why this would be a good idea. The key aspect is the balance between the costs of implementing an ISMS against the costs of suffering a serious attack on their information.

Property developers are keen to know where the Natterjack toad can be currently found so they can either avoid buying the land or, if they already have ownership of the land, possibly ‘remove’ the toad in advance of the planning applications being submitted to ‘avoid’ any problems with the approvals required. This information is on the website, which has no firewall protecting it.

It would cost GANT many thousands of pounds and several years of effort to reintroduce the toad to a habitat once it has been removed by either natural or man-made effects.

The funding for GANT is through members’ fees, grants from other nature conservancy organisations and commercial companies who make donations.

**ACTIVITY 1.2**

Consider three main areas where the chairperson should gather more detailed information to allow the committee to make reasonable judgements on whether or not it is sensible to carry out the ISMS implementation.

**SAMPLE QUESTIONS**

1. **If the accuracy of information is a major concern, which of the following would reflect that this is covered effectively?**
   a. Confidentiality.
   b. Integrity.
   c. Availability.
   d. None of these.

2. **When a user logs onto a computer system and is asked for their mother’s maiden name, which of the following aspects is the system ensuring?**
   a. Accountability.
   b. Authorisation.
   c. Authentication.
   d. Applicability.
3. ISO/IEC 27001 is an international standard for information security. Which organisation is responsible for its maintenance?
   a. The British Standards Institute.
   b. The government of the country in which it has been implemented.
   c. The European Union Standards Committee.
   d. The International Organization for Standardization.

4. How should the implementation of an information assurance system be seen within an organisation?
   a. As a problem for the IS department only to sort out.
   b. As a problem on which the senior managers should make a decision but then leave to others to deal with.
   c. As a whole-organisation issue.
   d. As an issue where outside expertise is the best solution.

5. How should the use of an international standard for information security be viewed by senior managers within an organisation?
   a. As a good idea if there was the right business environment in which to implement it.
   b. As implementing best practice.
   c. As overkill unless there are very serious problems with assurance.
   d. As the pet idea of the IT director who thinks it will look good to shareholders in the next annual report of the organisation.
INDEX

4G networks 133
5G networks 133, 138
A5 encryption 195
access control lists (ACLs) 135, 162
accidents 14, 20, 23, 69, 95, 97–8, 112–15
ACPO guidelines for computer-based evidence see National
Police Chiefs' Council (NPCC)
actions
avoid 4
mitigate 4
prevent 4
share 5
terminate 4
treat 4
active content 128
Active Cyber Defence strategy
205
activity solution pointers
215–29
Adobe Acrobat Reader 185
Advanced Encryption Standard
(AES) 195–6
algorithms 132, 138, 196, 199, 201
American National Standards
Institute (ANSI) 74
anti-virus software 23, 30, 32, 43,
128–9, 131, 162, 174
Apple® 74
Asimov, Isaac 12–13
assurance controls 41, 44, 53–7,
61–2, 69, 71–2
asymmetric digital subscriber
line (ADSL) 225
asymmetric model 197–8
asynchronous replication 180
attempted extortion 192
backdoors 72, 127
Bayesian statistical analysis 136,
140
Big Data 202
biometric identification 111, 134
Bishop, Sir Michael 22
Black Hat 204
blackmail 67, 71, 71–2, 192
Blancco Technology Group
172
block ciphers 195–6
blockchain services 201
Blowfish 195
Bluetooth ports 129
‘bots’ 127
Breach of Confidence 74
bring your own device (BYOD)
policy 12, 21, 133, 139, 172
Bromium Inc. 72
brown envelopes 183–4
bugs 94, 98, 131
Buncefield oil storage depot
disaster 20, 66, 145, 161, 181, 185
business continuity plans (BCPs)
180–1, 183–8
business fraud 71–2
business impact analysis (BIA)
24, 28, 33, 66, 178, 182, 186
business-to-business
transactions 12
Canadian Trusted Computer
Product Evaluation Criteria
(CTCPEC) 83
Capability Maturity Model (CMM)
97, 221
caveats 116–17
CDs 15, 128–9, 171
Centre for the Protection of
National Infrastructure (CPNI)
125, 192
Certificate in Information
Security Management Principles
(BCS) 8, 188
certification authorities (CAs) 77,
199–200
Certified Assisted Products
(CAPS) 84
Certified Cyber Professional
(CCP) 6–7
Certified Ethical Hacker (CEH) 145
Charities Commission 228
Chartered Institute of Information
Security (CIISec) 6
chief finance officers (CFOs) 41
chief information officers (CIOs)
41
chief information security
officers (CISO) 40–1
chief risk officers (CROs) 41
child pornography 44, 73, 192, 220
China State Council directive
273 78
Chinese walls 116
ciphertext 195–6
Civil Evidence Act (UK) 76
cloud access security brokers
(CASB) 136
cloud computing
cloud-based services 21, 97,
132, 134, 185–6
introduction 153–4
legal implications 154
nature of 226
selecting a supplier 155–6
supplier commercial and purchaser risk 157–8
Cloud Security Alliance (CSA) 158
code 98–9, 126
code of connection (CoCo) 62, 139
codes of ethics 56
Commercial Licensed Evaluation Facilities (CLEFs) 98
commercial off-the-shelf products (COTS) 94, 100
Commercial Product Assurance system (CPA) 84, 99
Committee of Sponsoring Organizations of the Treadway Commission (COSO) 57
Common Criteria certificates (CC) 84, 99
Common Criteria for Information Technology Security Evaluation Criteria (CC ITSEC) 83
Common Criteria Recognition Arrangement (CCRA) 84
Common Vulnerabilities and Exposures database (CVE) 204
Communications-Electronics Security Groups (CESG) 83–4
CESG Tailored Assurance Service (CTAS) 83–4
Companies Act (UK) 14, 42
Companies Audit, Investigations and Community Enterprise Act (2004) 56
computer aided instruction (CAI) see training delivery, computer-based (CBT)
computer emergency response teams (CERTs) 67, 192
Computer Fraud and Abuse Act 1984 (USA) 71
Computer Misuse Act 1990 71
contingency plans 15, 45
contractual threats 20
corrections 30
documentation, maintenance and testing 182–4
department for digital, culture, media and sports (DCMS) 12
department for homeland security (DHS) 192
digital certificates 138
digital shadows 203
digital signatures 198
Directive on computer misuse (EU) 71
disaster recovery (DR) business continuity plans (BCP) 177–9
documentation, maintenance and testing 182–4
incident management 187
management of services provision 184
off-site storage 185–6
personnel, suppliers and IT system providers 186–7
resilience and redundancy 179–80
writing and implementing plans 180–2
distributed control systems (DCSs) 145
distributed denial of service attacks (DDoS) 20, 67, 72
domain name systems (DNSs) 137
EAL 1 83, 99
EAL 4 84, 99
EAL 5–7 83, 99
Council of Registered Ethical Security Testers (CREST) 46, 145
countermeasures 4, 13, 15, 22, 96, 104, 115, 127–30, 149
cover time 196
crime
blackmail 67, 71, 71–2, 192
business fraud 71–2
cyber stalking 73
child pornography 44, 73, 192, 220
cyber terrorism 20, 64, 71, 126
deployment 71–2, 75, 202
espionage 20
extortion 67, 192
hacking 20, 71–2
identity theft 5, 20
information security 16
information theft 20
Internet 16
invoice fraud 16
obtaining information by deception 72
piracy 73–4
sexual grooming 73
theft 71
website defacement 72
cryptography
basic theory 194–5
cyber attack intelligence 202
hash functions 201
policies for cryptographic use 201–2
Pretty Good Privacy (PGP) 200–1
and privacy 78
public key (PKI) 197–200
regulation of controls 68
role of 194
secret, or symmetric, key 195–7
securing data exchange 149
threat intelligence see threat intelligence
cyber-attacks 12, 142, 180
Cyber Essentials scheme 84
Cyber Security Breaches Survey 2019 12
Cyber Security Information Sharing Partnership (CiSP) 204–5
cyber stalking 73
cyber terrorism 20, 64, 71, 126
dark web 203
data acquisition systems (SCADA) 145
Data Encryption Standard (DES) 196–7
Data Protection Act (DPA) 20, 42, 69, 111, 117, 151, 160, 185, 225–6
deception 71–2, 75, 202
defence in depth concept 62
demilitarised zones (DMZs) 115, 139, 149
Deming Cycle see Plan–Do–Check–Act (PDCA)
denial of service attacks (DoS) 20, 64, 110
department for digital, culture, media and sports (DCMS) 12
department for homeland security (DHS) 192
digital certificates 138
Digital Shadows 203
digital signatures 198
Directive on computer misuse (EU) 71
disaster recovery (DR) business continuity plans (BCP) 177–9
documentation, maintenance and testing 182–4
incident management 187
management of services provision 184
off-site storage 185–6
personnel, suppliers and IT system providers 186–7
resilience and redundancy 179–80
writing and implementing plans 180–2
distributed control systems (DCSs) 145
distributed denial of service attacks (DDoS) 20, 67, 72
domain name systems (DNSs) 137
EAL 1 83, 99
EAL 4 84, 99
EAL 5–7 83, 99
eavesdropping 20, 71, 148–9, 236
eBay 172
electronic data interchanges (EDIs) 138, 149
Electronic Identification, Authentication and Trust Services (eIDAS) 77
electronic signatures 77
emails 16, 107, 129–30, 162
encryption benefits of 224
GSM (2G) mobile 195
end-user code of practice see people security
enterprise IT 145
enterprise resource planning systems (ERP) 112, 145
espionage 20
ethics 6–7
European Commission 70, 84
European Free Trade Association (EFTA) 84
European Patent Convention (EPC) 75
European Telecommunications Standards Institute (ETSI) 84–5
European Union Agency for Network and Information Security (ENISA) 85, 122, 158
European Union (EU) 42, 44, 69–70, 74–5, 77–8, 84, 160
external services other organisations 151
protection of web services 149–50
real-time 147–8
securing data exchange 149
service management 152
extortion 67, 192
Fair and Accurate Credit Transaction Act 2003 (US) 73
Federal Bureau of Investigation (FBI) 126
Federal Information Processing Standards Publications (FIPS PUBS) 84
Federal Rules of Evidence (US) 76
Federal Trusted Computer System Evaluation Criteria (TCSECUS) 83
Financial Conduct Authority (FCA) 45, 82
Financial Services Act (FSA) 151
fingerprint identification 134, 187
firewalls 99, 115, 129–31, 133, 135–6, 139, 224
forensic investigation 16, 187
Forum for Incident Response and Security Teams (FIRST) 192
France 78, 84
Freedom of Information Act (FoIA) 71, 151
GATT, Trade Related Aspects of Intellectual Property Rights 1993 (GATT TRIPS) 74
GCHQ, Cheltenham 83, 197
General Data Protection Regulation (GDPR) 20, 42, 44–5, 67, 69–70, 73, 133, 135, 143, 151, 185, 225–6
Argentina 70
Canada 69–70
New Zealand 70
Switzerland 70
United Kingdom 70
Get Safe On-line (website) 122
Global Information Assurance Certification (GIAC) 145
Gnu PrivacyGuard 200
good practice guidelines (Business Continuity Institute) 188
GOVCERT (emergency response team) 192
Gramm-Leach-Bliley Act (GLBA) 69, 143
Grandfather-Father-Son system (GFS) 130, 160–1, 229
GSM (2G) mobile encryption 195
hacking 20, 25, 71–2, 115, 145
hashing 198–200
Health Insurance Portability and Accountability Act (HIPAA) 69, 135, 143
health and safety 14
HMRC 228
‘hole-in-the-wall’ cash dispensers 22
host intrusion detection systems (HIDSs) 161
https protocol 114
Human Rights Act (HRA) 70, 151
IAM Roadsmart 181
ID&A see user access controls, authentication and authorisation mechanisms
identity theft 5, 20
IdenTrust 200–1
incident investigation common processes 190–1
cryptography see cryptography
forensic services/third parties 190, 192–4
legal and regulatory guidelines 191
relations with law enforcement 191–2
Independent Evaluation for Assured Services (CAS) 84
indicators of compromise (IoCs) 203
industrial control systems (ICSs) 11, 145
information retrieval 5
security 6–7
information assurance (IA) business models 10–12
controls 4–5
international/national standards 8
management of 4
middle management 14–15
not an ‘add-on’ 10
policy 14
for the whole organisation 10
Information Commissioner’s Office (ICO) 45, 122
information and communications technology (ICT) 84
information risk accepting or tolerating 30
analysis 26–8
assessing in business terms 34
assets 22, 33
avoidance or termination 29
calculating 23–4
classification policies 33–4
communication and consultation 28
context establishment 25
cost against potential losses 34–5
identification 25–6
conformance with security policy 159
input correctness 160
installation of baseline controls 162
intrusion monitoring and detection methods 161–2
recovery capability 160–1
security documentation 163
separation of systems 158
IT Infrastructure Library (ITIL) 143, 188
just-in-time operations 12
Kegworth air crash 22–3
Kerberos 134, 201
key AES lengths 197
key exchange problem 197
key-logging 16, 114, 127
kopf unten (head-down generation) 139
legal framework
collection of admissible evidence 76–7
common concepts 71–3
contractual safeguards 75–6
copyright law 74
employment issues/employee rights 70–1
intellectual property rights (IPR) 74–5
introduction 67–8
protection of personal data 69–70
records retention 73–4
restrictions on purchase 78–9
securing digital signatures 77–8
line of business managers (LOB) 42
local area network (LAN) 136
local security co-ordinators 44
lottery win notifications 16
McGuire, Mike 72–3, 75
Maersk (shipping line) 142
malevolent cookies 127
malicious code see malicious software
Malicious Communications Act (UK) 73
malicious software
code of conduct 107
and common concepts of computer misuse 72
and disgruntled employees 175
and law enforcement 67
malware countermeasures 129–30
methods of control 130–2
and monitoring 91
now very sophisticated 51
and off-the-shelf products 94–5
and risks of unwanted code 98
routes of infection 128–39
security breaches 161
and security incident reporting 64
sheepdip scanners 130
subverting stored data 160
technical controls 126, 128–9
types 20, 126–8
malware see malicious software
management reviews 54
Markets in Financial Instruments Directive (MiFID) 151
masquerade attacks 198
message digest 198–9
Microsoft Office 365® 153
Microsoft® 74, 180
multi-factor authentication (MFA) 135
multi-protocol layer switching (MPLS) 136
National Counterintelligence and Security Center (US NCSC) 122
National Crime Agency (NCA) 67, 192
National Cyber Security Centre (NCSC) 6–7, 46, 67, 83, 84, 99, 192, 205
National Institute of Standards and Technology (NIST) 57
NIST Cybersecurity Framework 66, 84, 122, 125, 158, 204
operators of essential services (OESs) 42
not-Petya attack 142
Obscene Publications Act (UK) 73
Offensive Security Certified Professional (OSCP) 145
Official Secrets Act (OSA) 151
OKTA (cloud-based services) 134
onion model 103
Open Source Intelligence (OSI) 203
OpenIOC 204
OpenPGP 200
out of band authentication (OOB) 134
operators of essential services (OESs) 42
Outages 20
PACE/ACPO guidelines 193
paedophilia see crime
Pakistan 78
Pakistan Telecom Authority 78
‘passing off’ 74–5
passwords
developing standards, guidelines 48–52
hard-coded 162
one-time (OTPs) 111
and partitioning networks 135
protection 195
sharing 120
patches 98–9, 131, 162
patents 75
Payment Card Industry Data Security Standard requirements (PCI DSS) 57, 82, 135
payroll systems 112
Peabody, Jane 8, 123
PenTests 145–6
people security
acceptable use policies 107
codes of conduct 106–7
contracts of employment 104–5
organisational security culture 104
security awareness 105
segregation of duties 108
service contracts 106
third-party obligations 108–9
Personal Information Protection and Electronic Documentation Act (Canada) 69
personally identifiable information (PII) 69, 106, 154, 160, 172, 224
Peter, Laurence J. 170
phishing 16, 72
photocopiers 15
physical security
clear screen and desk policy 169–70
delivery and loading areas 173
description 103
introduction 166–7
moving property on and off site 170–2
protection of equipment 167–9
secure disposal procedures 172–3
tactical controls 174–5
PIN numbers 52, 110, 135
piracy 73–4
plaintext 195
Plan–Do–Check–Act Cycle (PDCA) 57, 91, 143–4
platform as a service (PaaS) 153–4, 155, 158
Police and Criminal Evidence Act (1984) 76, 190
Ponemon Institute report 142
privacy 69–70
Privacy Shield framework (US) 70
private automatic branch exchange systems (PABX) 148
procedures and people
general controls 102–4
introduction 102
people security see people security
security 103
training and awareness see training and awareness
user access controls see user access controls
professionalism 6–7
programme implementation
planning 58–9, 63
presenting positive benefits 60–1
security strategy and architecture 61–2
Protection from Harassment Act (UK) 73
ProtMon tools 140–1
public key infrastructure (PKI) 134–5, 197–200
Public Order Act (UK) 73
Public Records Acts 1957, 1967 (UK) 70
Publicly Available Specification 77 (PAS 77) 81, 188
Radius 134
ransomware 20, 67, 72–3, 127, 142, see also malicious software
Ratner, Gerald 22
Ratners jewellers 22
Recorded Future 203
Regulation of Investigatory Powers Act 2000 (RIPPA) 70
relevant digital service providers (RDSPs) 42
Request for Comments (RFCs) 84
retina identification 134
return on investment (ROI) 60
risk
acceptance 5
appetite 27
and corporate governance 14–15
countermeasures 13
description 3–4
do nothing option 5
during an audit or review 55
and life 13
and organisations 13
reduction 4
registers 27, 30, 35–6, 56
tolerance 5
transfer 4–5
risk assessments
and BIA 178
as part of design/development life cycle 95
qualitative 31
quantitative 32
questionnaires 32–3
results of 34
semi-quantitative 32
Risk Guidance 2014 (Financial Reporting Council) 35
road warriors 138
role-based access 113
Rolls-Royce 139
rootkits 127
RSA SecurID device 110, 199, 204
sabotage 20
SABSA matrix 143
sample questions 17–18, 36–7, 85–7, 100–1, 123–4, 164–5, 175–6, 206–7
SANS Institute 123
screen-scraping 16
secure sockets layer (SSL) 114
security
analytics 202
champions 42
forums 42
technical 103, 125
security incident management corporate systems 66
introduction 63–4
law enforcement 66–7
reporting, incident response teams/procedures 65–6
reporting, recording 64–5
security information and event management tools (SIEM) 92, 140–1, 203
security life cycles
information 88–90
monitoring system principles 91–2
systems development and support see systems development and support testing, audit and review 90–1
testing, links between IT and clerical processes 91
security operations centres (SOCs) 92, 136
Security Operations Maturity Architecture (SOMA) 57
security standards and procedures
certification of information security management systems 81–2
introduction 79
national and international standards 79–81
product certification 82–4
production of key technical standards 84–5
security training programmes 119–20
service level agreements (SLAs) 92
sexual grooming 73
SHA-256 199
shadow IT 138
single sign on systems (SSO) 134
slammer worm 127, 142
smart energy metering networks 196
smartphone zombies 139
smartphones 129
Snort (tool) 161
social engineering 20
Social Media Today 89
software as a service (SaaS) 21, 153, 155
sponsorship 119
spyware 127, 239
SSL cryptography 149
stand-by power generators 168–9
standby systems 179–80
Stateful Inspection (firewall) 141
steering committees 42
strategic controls 28
stream ciphers 195
Subject Access Requests 70
supply chains 187
symmetric encryption keys 138, 196, 199
synchronous replication 180
sysadmins 112–13
system misuse 108
systems development and support
accreditation 96
change control 96–7
commercial products 94
links with all business areas 94
preventing covert channels 98
security of acceptance processes 95–6
security issues from outsourcing 97
security patching 98–9
security requirement specification 93
separation of development/live systems 95
system and product assessment 93–4
use of escrow 99–100
target of evaluation (ToE) 83
Target (retailer) 139
Telecommunications Directive (UK) 70
terrorist activity 192
theft 71
threat intelligence
co-operative 204–5
cyber (CTI) 203–4
introduction 202–3
and vulnerability data 202
Tiger Scheme certifications 145
TLS cryptography 137, 149, 196–7, 229
training and awareness
approaches to 119–20
available materials 120–2
information sources 122–3
introduction 117–18
purpose 118–19
training delivery
computer-based (CBT) 121
electronic formats 121
escape rooms 121
external 120
face-to-face 120
videos 120–1
transport layer security (TLS) 132
Triple-Data Encryption Standard (Triple-DES) 195
Trojans 127–9, 135
Turnbull Report (1999) 14, 35, 42
two-factor authentication (2FA) 110
United States Department of Commerce 70
USB memory sticks 15, 128–9
user access controls
access points 114–15
administration 113–14
authentication and authorisation mechanisms 109–11, 114, 116, 135, 139, 150
data protection 115
effective use of 111–13
video-conferencing 148, 225
virtual private networks (VPNs) 114, 132–3, 136, 139, 149–50, 229
viruses 20, 32, 126–7
voice over internet protocol (VOIP) 148
vulnerabilities 3, 90–1, 146, 215
Wannacry ransomware virus 127, 180
war chests 185
war dialling 148
Wassenaar Arrangement 1996 (WA) '98
website defacement 72
websites 127–31
wide area network (WAN) 136
Wi-Fi protected access protocol (WPA) 148
WikiLeaks 142
wired equivalent privacy protocol (WEP) 148
wireless access points (WAP) 134
wireless networks 114–15, 133, 136, 148
Wireshark (software) 135, 145
World Standards Cooperation 80
World Trade Center incident, New York 181, 185
worms 127, 129
WPA3 134
YouTube 122
zero-day exploits 128
INFORMATION SECURITY MANAGEMENT PRINCIPLES
Third edition
Andy Taylor (editor), David Alexander, Amanda Finch, David Sutton

Information is one of the currencies of today’s society. As access to fast, reliable data at work and at home becomes increasingly essential to day to day operations, new risks emerge which threaten the very information that enables businesses and helps society to function.

By focusing on the three main areas of information assurance – confidentiality, integrity and availability – this book gives you the skills to identify information security threats and protect yourself and your business against them.

- Understand information threats and vulnerabilities and implement countermeasures against these
- Manage emerging risks to your data
- Learn information assurance best practice from experienced authors
- Supports BCS certification in Information Security Management Principles

ABOUT THE AUTHORS
The authors are at the forefront of information security and are instrumental in shaping policy and implementing best practice. They have gained considerable experience across a wide range of public and private sector bodies including the Home Office, MoD, RAF, Royal Navy, British Airways, Marks & Spencer and O2.

Fantastic for those studying information security management and as a desk-side reference...refreshingly understandable.
Helen Mary Jones, Group Information Security Manager, The Jockey Club

An excellent introduction to information security. Highly recommended.
John Hughes, InfoSec Skills

Review of previous edition

You might also be interested in:

Information Technology, Management

Cover photo: iStock ID SteveMcSweeny

ISBN 978-1-78017-518-8

Paperback available