

CONTENTS

Introduction 1

01 Why is information security necessary? 9

The nature of information security threats 10
Information insecurity 12
Impacts of information security threats 13
Cybercrime 14
Cyberwar 15
Advanced persistent threat 16
Future risks 16
Legislation 19
Benefits of an information security management system 20

02 The UK Combined Code, the Turnbull Report and Sarbanes–Oxley 23

The Combined Code 23
The Turnbull Report 24
The Revised Combined Code 25
Sarbanes–Oxley 28
Enterprise risk management 30
Regulatory compliance 32
IT governance 33

03 ISO27001 35

Benefits of certification 35
The history of ISO27001 and ISO27002 36
The ISO/IEC 27000 series of standards 37
Use of the standard 38
ISO/IEC 27002 39
The Plan–Do–Check–Act and process approach 40
Structured approach to implementation 41
Quality system integration 43
Documentation 44
Continual improvement and metrics 48

04	Organizing information security	51
	Internal organization	52
	Management review	54
	The information security manager	54
	The cross-functional management forum	56
	The ISO27001 project group	57
	Approval process for information processing facilities	62
	Specialist information security advice	63
	Contact with authorities and special interest groups	66
	Independent review of information security	67
	Summary	68
05	Information security policy and scope	69
	Information security policy	69
	A policy statement	75
	Costs and the monitoring of progress	76
06	The risk assessment and Statement of Applicability	79
	Establishing security requirements	79
	Risks, impacts and risk management	79
	Selection of controls and Statement of Applicability	92
	Gap analysis	96
	Risk assessment tools	96
	Risk treatment plan	97
	Measures of effectiveness	98
07	External parties	101
	Identification of risks related to external parties	101
	Types of access	103
	Reasons for access	104
	Outsourcing	105
	On-site contractors	107
	Addressing security when dealing with customers	108
	Addressing security in third-party agreements	109
08	Asset management	113
	Asset owners	113
	Inventory	114
	Acceptable use of assets	117

	Information classification	117
	Unified classification markings	120
	Government classification markings	121
	Information lifecycle	122
	Information labelling and handling	122
	Non-disclosure agreements and trusted partners	127
09	Human resources security	129
	Job descriptions and competency requirements	129
	Screening	131
	Terms and conditions of employment	134
	During employment	135
	Disciplinary process	141
	Termination or change of employment	141
10	Physical and environmental security	145
	Secure areas	145
	Public access, delivery and loading areas	153
11	Equipment security	155
	Equipment siting and protection	155
	Supporting utilities	158
	Cabling security	159
	Equipment maintenance	161
	Security of equipment off-premises	161
	Secure disposal or reuse of equipment	162
	Removal of property	163
12	Communications and operations management	165
	Documented operating procedures	165
	Change management	167
	Segregation of duties	168
	Separation of development, test and operational facilities	168
	Third-party service delivery management	169
	Monitoring and review of third-party services	171
	Managing changes to third-party services	172
	System planning and acceptance	173

- 13 Controls against malicious software (malware) and back-ups 177**
 - Viruses, worms and Trojans 177
 - Spyware 179
 - Anti-malware software 179
 - Hoax messages 180
 - Phishing and pharming 181
 - Anti-malware controls 182
 - Airborne viruses 184
 - Controls against mobile code 185
 - Back-up 186
- 14 Network security management and media handling 191**
 - Network management 191
 - Media handling 193
- 15 Exchanges of information 197**
 - Information exchange policies and procedures 197
 - Exchange agreements 200
 - Physical media in transit 201
 - Business information systems 202
- 16 E-commerce services 205**
 - E-commerce issues 205
 - Security technologies 208
 - Server security 210
 - Online transactions 211
 - Publicly available information 212
- 17 E-mail, internet use and social media 215**
 - Security risks in e-mail 215
 - Spam 217
 - Misuse of the internet 218
 - Internet acceptable use policy 220
 - Social media 222
- 18 Access control 223**
 - Hackers 223
 - Hacker techniques 224

- System configuration 228
- Access control policy 228
- User access management 230
- Clear desk and clear screen policy 239
- 19 Network access control 241**
 - Networks 241
 - Network security 245
 - Server virtualization 251
- 20 Operating system access control 253**
 - Secure log-on procedures 253
 - User identification and authentication 254
 - Password management system 255
 - Use of system utilities 255
 - Session time-out 256
 - Limitation of connection time 256
- 21 Application access control and teleworking 259**
 - Application and information access control 259
 - Mobile computing and teleworking 261
 - Teleworking 263
- 22 Systems acquisition, development and maintenance 267**
 - Security requirements analysis and specification 267
 - Correct processing in applications 268
- 23 Cryptographic controls 273**
 - Encryption 274
 - Public key infrastructure 275
 - Digital signatures 276
 - Non-repudiation services 277
 - Key management 277
- 24 Security in development and support processes 279**
 - System files 279
 - Access control to program source code 280
 - Development and support processes 281
 - Vulnerability management 284

- 25 Monitoring and information security incident management 287**
- Monitoring 287
 - Information security events 291
 - Management of information security incidents and improvements 296
 - Legal admissibility 301
- 26 Business continuity management 303**
- ISO22301 303
 - The business continuity management process 304
 - Business continuity and risk assessment 305
 - Developing and implementing continuity plans 306
 - Business continuity planning framework 308
 - Testing, maintaining and reassessing business continuity plans 312
- 27 Compliance 315**
- Identification of applicable legislation 315
 - Intellectual property rights 328
 - Safeguarding of organizational records 332
 - Data protection and privacy of personal information 333
 - Prevention of misuse of information processing facilities 335
 - Regulation of cryptographic controls 335
 - Compliance with security policies and standards 336
 - Information systems audit considerations 338
- 28 The ISO27001 audit 341**
- Selection of auditors 341
 - Initial audit 342
 - Preparation for audit 343
 - Terminology 345
- Appendix 1: Useful websites 347*
- Appendix 2: Further reading 353*
- Index 357*