

CONTENTS

About the author xi

Introduction 1

1 Why is information security necessary? 9

The nature of information security threats 10

Information insecurity 12

Impacts of information security threats 13

Cybercrime 14

Cyberwar 16

Advanced persistent threat 17

Future risks 17

Legislation 20

Benefits of an information security management system 22

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

The Combined Code 23

The Turnbull Report 24

The Corporate Governance Code 25

Sarbanes–Oxley 29

Enterprise risk management 31

Regulatory compliance 33

IT governance 34

3 ISO27001 37

Benefits of certification 37

The history of ISO27001 and ISO27002 38

The ISO/IEC 27000 series of standards 40

Use of the standard 41

ISO/IEC 27002 42

Continual improvement, Plan–Do–Check–Act, and process approach 43

	Structured approach to implementation	44
	Management system integration	47
	Documentation	48
	Continual improvement and metrics	53
4	Organizing information security	55
	Internal organization	56
	Management review	58
	The information security manager	59
	The cross-functional management forum	61
	The ISO27001 project group	62
	Specialist information security advice	68
	Segregation of duties	70
	Contact with special interest groups	71
	Contact with authorities	73
	Information security in project management	73
	Independent review of information security	74
	Summary	75
5	Information security policy and scope	77
	Context of the organization	77
	Information security policy	78
	A policy statement	85
	Costs and the monitoring of progress	86
6	The risk assessment and Statement of Applicability	89
	Establishing security requirements	89
	Risks, impacts and risk management	89
	Cyber Essentials	99
	Selection of controls and Statement of Applicability	106
	Statement of Applicability Example	108
	Gap analysis	109
	Risk assessment tools	110
	Risk treatment plan	111
	Measures of effectiveness	112
7	Mobile devices	115
	Mobile devices and teleworking	115
	Teleworking	118

8 Human resources security 121

Job descriptions and competency requirements 121

Screening 123

Terms and conditions of employment 126

During employment 128

Disciplinary process 134

Termination or change of employment 135

9 Asset management 139

Asset owners 139

Inventory 140

Acceptable use of assets 143

Information classification 144

Unified classification markings 146

Government classification markings 148

Information lifecycle 149

Information labelling and handling 150

Non-disclosure agreements and trusted partners 155

10 Media handling 157

Physical media in transit 159

11 Access control 161

Hackers 161

Hacker techniques 162

System configuration 166

Access control policy 167

Network Access Control 169

12 User access management 179

User access provisioning 184

13 System and application access control 191

Secure log-on procedures 192

Password management system 193

Use of privileged utility programs 194

Access control to program source code 195

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

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

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

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

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

	Technical vulnerability management	250
	Information Systems Audits	252
19	Communications management	253
	Network security management	253
20	Exchanges of information	259
	Information transfer policies and procedures	259
	Agreements on information transfers	262
	E-mail and social media	263
	Security risks in e-mail	264
	Spam	266
	Misuse of the internet	267
	Internet acceptable use policy	269
	Social media	271
21	System acquisition, development and maintenance	273
	Security requirements analysis and specification	273
	Securing application services on public networks	274
	E-commerce issues	275
	Security technologies	278
	Server security	281
	Server virtualization	282
	Protecting application services transactions	283
22	Development and support processes	285
	Secure development policy	285
	Secure systems engineering principles	289
	Secure development environment	289
	Security and acceptance testing	290
23	Supplier relationships	295
	Information security policy for supplier relationships	295
	Addressing security within supplier agreements	297
	ICT supply chain	299
	Monitoring and review of supplier services	301
	Managing changes to supplier services	302

24	Monitoring and information security incident management	305
	Logging and monitoring	305
	Information security events and incidents	310
	Incident management – responsibilities and procedures	310
	Reporting information security events	313
	Reporting software malfunctions	316
	Assessment of and decision on information security events	318
	Response to information security incidents	318
	Legal admissibility	321
25	Business and information security continuity management	323
	ISO22301	323
	The business continuity management process	324
	Business continuity and risk assessment	325
	Developing and implementing continuity plans	327
	Business continuity planning framework	328
	Testing, maintaining and reassessing business continuity plans	332
	Information security continuity	335
26	Compliance	339
	Identification of applicable legislation	340
	Intellectual property rights	353
	Protection of organizational records	358
	Privacy and protection of personally identifiable information	359
	Regulation of cryptographic controls	361
	Compliance with security policies and standards	361
	Information systems audit considerations	364
27	The ISO27001 audit	365
	Selection of auditors	365
	Initial audit	367
	Preparation for audit	368
	Terminology	371
	<i>Appendix 1: Useful websites</i>	<i>373</i>
	<i>Appendix 2: Further reading</i>	<i>379</i>
	<i>Index</i>	<i>395</i>