Contents

Foreword by Nigel Turnbull *xi*

How to use this book *xiii*

Acknowledgements *xv*

Introduction **1**

The information economy 2

What is IT governance? 3

Information security 4

1. Why is information security necessary? **9**

Nature of information security threats 10

Prevalence of information security threats 11

Impacts of information security threats 13

Cybercrime 15

Cyberwar 17

Future risks 18

Legislation 21

Benefits of an information security management system 22

2. **The Combined Code, the Turnbull Report and Sarbanes-Oxley** **23**
The Combined Code 23
The Turnbull Report 24
Revised Combined Code 25
Sarbanes-Oxley 28
IT governance 30

3. **BS 7799** **33**
Benefits of certification 33
History of BS 7799 and ISO/IEC 17799 35
Use of the standard 36
ISO/IEC 17799 36
PDCA and process approach 38
Structured approach to implementation 39
Quality system integration 41
Documentation 42
Continual improvement and metrics 46

4. **Organizing information security** **49**
Internal organization 50
Management review 51
Information security manager 51
The cross-functional management forum 53
BS 7799 project group 54
Approval process for information processing facilities 59
Product selection and the Common Criteria 60
Specialist information security advice 61
Contact with authorities and special interest groups 66
Independent review of information security 67
Summary 68

5. **Information security policy and scope** **69**
Information security policy 69
A policy statement 75
Costs and monitoring progress 77

6. **The risk assessment and statement of applicability** **79**
Establishing security requirements 79
Risks, impacts and risk management 80
Selection of controls and statement of applicability 93
Gap analysis 96
Risk assessment tools 96
Risk treatment plan 97

7. External parties **99**
Identification of risks related to external parties 99
Types of access 101
Reasons for access 102
Outsourcing 103
On-site contractors 105
Addressing security when dealing with customers 106
Addressing security in third party agreements 107

8. Asset management **111**
Asset owners 111
Inventory 112
Acceptable use of assets 115
Information classification 115
Unified classification markings 118
Information labelling and handling 120
Non-disclosure agreements and trusted partners 125

9. Human resources security **127**
Job descriptions and competence requirements 128
Screening 129
Terms and conditions of employment 132
During employment 134
Disciplinary process 139
Termination or change of employment 140

10. Physical and environmental security **143**
Secure areas 143
Public access, delivery and loading areas 151

11. Equipment security **153**
Equipment siting and protection 153
Supporting utilities 156
Cabling security 158
Equipment maintenance 159
Security of equipment off-premises 160
Secure disposal or reuse of equipment 161
Removal of property 161

12. Communications and operations management **163**
Documented operating procedures 163
Change management 165
Segregation of duties 166
Separation of development, test and operational facilities 167

Third party service delivery management 168
Monitoring and review of third party services 169
Managing changes to third party services 170
System planning and acceptance 171

13. Controls against malicious software (malware) and back-ups 177
Viruses, worms and Trojans 177
Spyware 179
Anti-malware software 179
Hoax messages 180
Anti-malware controls 181
Airborne viruses 184
Controls against mobile code 185
Back-up 185

14. Network security management and media handling 189
Network management 189
Media handling 192

15. Exchanges of information 195
Information exchange policies and procedures 195
Exchange agreements 198
Physical media in transit 199
Business information systems 199

16. Electronic commerce services 203
E-commerce issues 203
Security technologies 206
Server security 208
Online transactions 209
Publicly available information 210

17. E-mail and internet use 213
Security risks in e-mail 214
Spam 216
Misuse of the internet 216
Internet acceptable use policy (AUP) 218

18. Access control 221
Hackers 221
Hacker techniques 222
System configuration 225
Access control policy 225

User access management 228
Clear desk and clear screen policy 236

19. Network access control 239
Networks 239
Network security 243

20. Operating system access control 251
Secure log-on procedures 251
User identification and authentication 253
Password management system 253
Use of system utilities 254
Session time-out 254
Limitation of connection time 255

21. Application access control and teleworking 257
Application and information access control 257
Mobile computing and teleworking 259

22. Systems acquisition, development and maintenance 265
Security requirements analysis and specification 265
Correct processing in applications 266

23. Cryptographic controls 271
Encryption 272
Public key infrastructure (PKI) 273
Digital signatures 274
Non-repudiation services 275
Key management 275

24. Security in development and support processes 279
System files 279
Access control to program source code 281
Development and support processes 281
Vulnerability management 285

25. Monitoring and information security incident management 287
Monitoring 287
Information security events 292
Management of information security incidents and improvements 297

26. Business continuity management 303
Business continuity management process 304
Business continuity and risk assessment 305

Developing and implementing continuity plans 306
Business continuity planning framework 307
Testing, maintaining and reassessing business continuity plans 311

27. **Compliance** **315**
Identification of applicable legislation 316
Intellectual property rights (IPR) 324
Safeguarding of organizational records 328
Data protection and privacy of personal information 330
Prevention of misuse of information processing facilities 331
Regulation of cryptographic controls 331
Compliance with security policies and standards 332
Information systems audit considerations 335

28. **The BS 7799 audit** **337**
Selection of auditors 337
Initial visit 339
Preparation for audit 340

Appendices **343**

I. **Useful websites** **345**
IT governance 345
BS 7799 certification organizations 345
E-learning 346
Microsoft 346
Information security 346
Accounting, finance and economics 349
Business, management and governance 350
Contingency planning and disaster recovery 350
Information technology 351
Risk management 352

II. **ISO/IEC 17799:2005** **353**

III. **Further reading** **355**

Index *357*