Table of Contents

PREFACE xv
FOREWORD xxiii

CHAPTER 1
Introduction to the Management of Information Security 1

Introduction 2
What Is Security? 3
CNSS Security Model 5
Key Concepts of Information Security 6
What Is Management? 8
Behavioral Types of Leaders 8
Management Characteristics 9
Solving Problems 11
Principles of Information Security Management 13
Planning 13
Policy 14
Programs 14
Protection 15
People 15
Projects 15
Project Management 15
Applying Project Management to Security 17
PMBoK Knowledge Areas 18
Project Management Tools 25
Work Breakdown Structure 25
Task-Sequencing Approaches 26
Automated Project Tools 30
Chapter Summary 30
Review Questions 31
Exercises 32
Closing Case 32
Endnotes 33

CHAPTER 2
Planning for Security 35

Introduction 37
The Role of Planning 37
Precursors to Planning 38
Values Statement 39
Vision Statement 40
Mission Statement 40
Strategic Planning 41
Creating a Strategic Plan 42
Planning Levels 42
Planning and the CISO 43
Information Security Governance 45
Desired Outcomes 45

Benefits of Information Security Governance . . . 46
Implementing Information Security Governance . . . 47
Security Convergence . . . 47
Planning for Information Security Implementation . . . 50
Introduction to the Security Systems Development Life Cycle . . . 54
Chapter Summary . . . 67
Review Questions . . . 68
Exercises . . . 69
Closing Case . . . 69
Endnotes . . . 70

CHAPTER 3
Planning for Contingencies . . . 73
Introduction . . . 74
Fundamentals of Contingency Planning . . . 75
Components of Contingency Planning . . . 79
Business Impact Analysis . . . 79
Contingency Planning Policies . . . 85
Incident Response . . . 85
Disaster Recovery . . . 97
Business Continuity . . . 107
Crisis Management . . . 111
Business Resumption . . . 113
Testing Contingency Plans . . . 115
Final Thoughts . . . 117
Chapter Summary . . . 117
Review Questions . . . 118
Exercises . . . 119
Closing Case . . . 120
Endnotes . . . 120

CHAPTER 4
Information Security Policy . . . 123
Introduction . . . 124
Why Policy? . . . 125
Policy, Standards, and Practices . . . 127
Enterprise Information Security Policy . . . 129
Integrating an Organization's Mission and Objectives into the EISP . . . 129
EISP Elements . . . 129
Example EISP Components . . . 130
Issue-Specific Security Policy . . . 134
Components of the ISSP . . . 135
Implementing the ISSP . . . 137
System-Specific Security Policy . . . 138
Managerial Guidance SysSPs . . . 138
Technical Specification SysSPs . . . 140
Guidelines for Effective Policy . . . 143

Developing Information Security Policy . . . 143
Policy Distribution . . . 148
Policy Reading . . . 149
Policy Comprehension . . . 149
Policy Compliance . . . 150
Policy Enforcement . . . 150

The Information Securities Policy Made Easy Approach . . . 152
Checklist of Steps in the Policy Development Process . . . 152
Next Steps . . . 154

SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems . . . 154

A Final Note On Policy . . . 155

Chapter Summary . . . 156

Review Questions . . . 157

Exercises . . . 157

Closing Case . . . 158

Endnotes . . . 159

CHAPTER 5
Developing the Security Program . . . 161

Introduction . . . 162

Organizing for Security . . . 163
Security in Large Organizations . . . 165
Security in Medium-Sized Organizations . . . 170
Security in Small Organizations . . . 170

Placing Information Security within an Organization . . . 171
Option 1: Information Technology . . . 174
Option 2: Security . . . 175
Option 3: Administrative Services . . . 176
Option 4: Insurance and Risk Management . . . 177
Option 5: Strategy and Planning . . . 179
Other Options . . . 180
Summary of Reporting Relationships . . . 181

Components of the Security Program . . . 181

Information Security Roles and Titles . . . 185
Chief Information Security Officer . . . 185
Security Managers . . . 186
Security Administrators and Analysts . . . 187
Security Technicians . . . 187
Security Staffers and Watchstanders . . . 187
Security Consultants . . . 188
Security Officers and Investigators . . . 188
Help Desk Personnel . . . 188

Implementing Security Education, Training, and Awareness Programs . . . 188
Security Education . . . 189
Security Training . . . 193
Training Techniques . . . 195
Identify Program Scope, Goals, and Objectives . . . 197
Identify Training Staff . . . 197
Identify Target Audiences . . . 197
Motivate Management and Employees . . . 197
Administer the Program . . . 198
Maintain the Program . . . 198

Evaluate the Program . . . 198
Security Awareness . . . 199
Chapter Summary . . . 206
Review Questions . . . 207
Exercises . . . 208
Closing Case . . . 209
Endnotes . . . 209

CHAPTER 6
Security Management Models . . . 211
Introduction . . . 212
Blueprints, Frameworks, and Security Models . . . 212
Access Control Models . . . 213
Categories of Access Control . . . 214
Security Architecture Models . . . 219
Trusted Computing Base . . . 220
Information Technology System Evaluation Criteria . . . 221
The Common Criteria . . . 221
Bell-LaPadula Confidentiality Model . . . 222
Biba Integrity Model . . . 223
Clark-Wilson Integrity Model . . . 223
Graham-Denning Access Control Model . . . 224
Harrison-Ruzzo-Ullman Model . . . 224
Brewer-Nash Model (Chinese Wall) . . . 225
Security Management Models . . . 225
The ISO 27000 Series . . . 225
NIST Security Models . . . 229
Control Objectives for Information and Related Technology . . . 236
Committee of Sponsoring Organizations . . . 238
Information Technology Infrastructure Library . . . 239
Information Security Governance Framework . . . 239
Chapter Summary . . . 241
Review Questions . . . 242
Exercises . . . 243
Closing Case . . . 243
Endnotes . . . 244

CHAPTER 7
Security Management Practices . . . 247
Introduction . . . 248
Benchmarking . . . 248
Standards of Due Care/Due Diligence . . . 249
Recommended Security Practices . . . 249
Selecting Recommended Practices . . . 252
Limitations to Benchmarking and Recommended Practices . . . 253
Baselining . . . 254
Support for Benchmarks and Baselines . . . 254
Performance Measurement in InfoSec Management . . . 257
InfoSec Performance Management . . . 257

Information Security Metrics . . . 258
Building the Performance Measurement Program . . . 259
Specifying InfoSec Measurements . . . 260
Collecting InfoSec Measurements . . . 261
Implementing InfoSec Performance Measurement . . . 265
Reporting InfoSec Performance Measurements . . . 266

Trends in Certification and Accreditation . . . 268
NIST SP 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach . . . 268

Chapter Summary . . . 274

Review Questions . . . 275

Exercises . . . 275

Closing Case . . . 276

Endnotes . . . 277

CHAPTER 8
Risk Management: Identifying and Assessing Risk . . . 279

Introduction . . . 280

Risk Management . . . 280
Knowing Yourself . . . 281
Knowing the Enemy . . . 281
Accountability for Risk Management . . . 281

Risk Identification . . . 282
Creating an Inventory of Information Assets . . . 283
Classifying and Categorizing Assets . . . 287
Assessing Values for Information Assets . . . 288
Listing Assets in Order of Importance . . . 290
Threat Identification . . . 291
Methods of Assessing Threats . . . 295
The TVA Worksheet . . . 298

Risk Assessment . . . 300
Introduction to Risk Assessment . . . 301
Likelihood . . . 301
Assessing Potential Loss . . . 302
Percentage of Risk Mitigated by Current Controls . . . 302
Uncertainty . . . 302
Risk Determination . . . 302
Likelihood and Consequences . . . 303
Identify Possible Controls . . . 305
Access Controls . . . 305

Documenting the Results of Risk Assessment . . . 305

Chapter Summary . . . 307

Review Questions . . . 309

Exercises . . . 309

Closing Case . . . 310

Endnotes . . . 311

CHAPTER 9
Risk Management: Controlling Risk . . . 313

Introduction . . . 314

Risk Control Strategies . . . 315
Defense . . . 315
Transferal . . . 316
Mitigation . . . 316
Acceptance . . . 316
Termination . . . 318
Managing Risk . . . 318
Feasibility and Cost-Benefit Analysis . . . 321
Cost-Benefit Analysis . . . 321
Other Methods of Establishing Feasibility . . . 326
Alternatives to Feasibility Analysis . . . 328
Recommended Risk Control Practices . . . 331
Qualitative and Hybrid Measures . . . 331
Delphi Technique . . . 332
The OCTAVE Methods . . . 332
Microsoft Risk Management Approach . . . 332
FAIR . . . 333
ISO 27005 Standard for InfoSec Risk Management . . . 334
NIST Risk Management Model . . . 334
Other Methods . . . 337
Chapter Summary . . . 338
Review Questions . . . 338
Exercises . . . 339
Closing Case . . . 341
Endnotes . . . 341

CHAPTER 10
Protection Mechanisms . . . 343

Introduction . . . 345
Access Controls . . . 346
Identification . . . 346
Authentication . . . 346
Authorization . . . 353
Accountability . . . 354
Managing Access Controls . . . 358
Firewalls . . . 358
The Development of Firewalls . . . 358
Firewall Architectures . . . 361
Selecting the Right Firewall . . . 364
Managing Firewalls . . . 365
Intrusion Detection and Prevention Systems . . . 367
Host-Based IDPS . . . 367
Network-Based IDPS . . . 368
Signature-Based IDPS . . . 369
Anomaly-Based IDPS . . . 369
Managing Intrusion Detection and Prevention Systems . . . 369
Remote Access Protection . . . 370
RADIUS and TACACS . . . 371
Managing Dial-Up Connections . . . 372
Wireless Networking Protection . . . 372
Wired Equivalent Privacy (WEP) . . . 373
Wi-Fi Protected Access (WPA) . . . 373
WiMax . . . 373

Bluetooth 374
Managing Wireless Connections 374
Scanning and Analysis Tools 375
Port Scanners 376
Vulnerability Scanners 377
Packet Sniffers 377
Content Filters 377
Trap and Trace 378
Managing Scanning and Analysis Tools 378
Cryptography 379
Encryption Operations 381
Using Cryptographic Controls 388
Managing Cryptographic Controls 391
Chapter Summary 393
Review Questions 394
Exercises 395
Closing Case 395
Endnotes 397

CHAPTER 11
Personnel and Security 399
Introduction 401
Staffing the Security Function 401
Qualifications and Requirements 402
Entering the Information Security Profession 402
Information Security Positions 403
Information Security Department Manager 405
Information Security Engineer 412
Information Security Professional Credentials 415
$(ISC)^2$ Certifications 416
ISACA Certifications 419
SANS Certifications 422
EC-Council Certifications 423
CompTIA Certifications 424
ISFCE Certifications 424
Certification Costs 425
Employment Policies and Practices 426
Hiring 428
Contracts and Employment 430
Security as Part of Performance Evaluation 430
Termination Issues 430
Personnel Security Practices 432
Security of Personnel and Personal Data 433
Security Considerations for Nonemployees 434
Chapter Summary 439
Review Questions 440
Exercises 441
Closing Case 441
Endnotes 442

CHAPTER 12
Law and Ethics **445**
Introduction 446
Law and Ethics in InfoSec 447
InfoSec and the Law 447
Types of Law 447
Relevant U.S. Laws 447
International Laws and Legal Bodies 462
State and Local Regulations 463
Policy versus Law 466
Ethics in InfoSec 466
Ethics and Education 470
Deterring Unethical and Illegal Behavior 472
Professional Organizations and their Codes of Ethics 473
Association for Computing Machinery (ACM) 473
International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ 473
SANS 474
Information Systems Audit and Control Association (ISACA) 474
Information Systems Security Association (ISSA) 475
Organizational Liability and the Need for Counsel 476
Key Law Enforcement Agencies 476
Managing Investigations in the Organization 478
Digital Forensics Team 480
Affidavits and Search Warrants 480
Digital Forensics Methodology 480
Evidentiary Procedures 483
Chapter Summary 483
Review Questions 484
Exercises 485
Closing Case 486
Endnotes 486

APPENDIX
NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems **489**
ISO 17799: 2005 Overview 514
The OCTAVE Method of Risk Management 519
Microsoft Risk Management Approach 526

GLOSSARY **533**
INDEX **545**