



Auerbach Publications
Taylor & Francis Group

COMPLETE GUIDE
TO
CISM[®]
CERTIFICATION

THOMAS R. PELTIER
JUSTIN PELTIER

Contents

Preface	xv
About the Authors	xvii
1 Information Security Governance	1
Functional Area Overview	1
CISM® Mapping	2
Introduction	2
Developing an Information Security Strategy in Support of Business Strategy and Direction	4
Obtain Senior Management Commitment and Support	12
Definitions of Roles and Responsibilities	14
Obtaining Senior Management Commitment	15
Change in Focus	16
Responsibilities and Functional Roles	17
Where Not to Report	17
Recommendation	19
Establish Reporting Communications That Support Information Security Governance Activities	19
Mission Statement	23
Legal and Regulatory Issues	24
Establish and Maintain Information Security Policies	32
Global Policy (Tier 1)	33
Topic	34
Scope	34
Responsibilities	35
Compliance or Consequences	35
Topic-Specific Policy (Tier 2)	35
Thesis Statement	36
Relevance	36
Responsibilities	37

Compliance	37
Supplementary Information	37
Application-Specific Policy (Tier 3)	38
Key Security Concepts	39
Ensure the Development of Procedures and Guidelines That	
Support the Information Security Policy	39
Develop Business Case and Enterprise Value Analysis Support	41
Summary	45
What Was Covered in This Chapter	45
Questions	45
2 Information Security Risk Management	53
Functional Area Overview	53
CISM Mapping	54
Introduction	54
Develop a Systematic and Continuous Risk Management Process	58
Ensure Risk Identification, Analysis, and Mitigation Activities	
Are Integrated Into the Life Cycle Process	60
Apply Risk Identification and Analysis Methods	66
Step 1: Asset Definition	67
Step 2: Threat Identification	69
Step 3: Determine Probability of Occurrence	72
Step 4: Determine the Impact of the Threat	72
Step 5: Controls Recommended	74
Step 6: Documentation	75
Cost-Benefit Analysis	75
Define Strategies and Prioritize Options to Mitigate Risks to	
Levels Acceptable to the Enterprise	87
Step 1: Threat Identification	91
Step 2: Threat Vulnerability	93
Step 3: Controls and Safeguards	98
Step 4: Cost-Benefit Analysis	101
Step 5: Documentation	114
Quantitative Versus Qualitative Risk Assessment	118
Report Significant Changes in Risk	121
Knowledge Statements	122
Gap Analysis	122
Recovery Time Objectives	123
Data (Information) Classification	123
Summary	125
What Was Covered in This Chapter	125
Questions	126
3 Information Security Program Management	133
Functional Area Overview	133
CISM Mapping	133

Introduction	134
The OSI Model	134
Layer 1: Physical	135
Layer 2: Data Link	135
Layer 3: Network	136
Layer 4: Transport	138
Layer 5: Session	139
Layer 6: Presentation	139
Layer 7: Application	139
The TCP/IP Model	141
IP Addressing	142
Protocols	146
Internet Protocol (IP) Details	147
Internet Protocol (IP) Network and Host	147
Subnet Masks and Internet Protocol (IP) Classes	148
Class A Networks	148
Class B Networks	148
Class C Networks	148
Beyond Class C Networks	149
IP Address Availability and Internet Protocol (IP) Version 6	149
IP Hosts	150
Private Internet Protocol (IP) Networks	152
Network Address Translation (NAT)	152
The Internet Protocol (IP) Header	153
Datagram Structure	156
Transmission Control Protocol (TCP)	159
TCP Ports	159
Well-Known Ports	160
Registered Ports	160
Dynamic Ports	160
Port Scanning	163
The TCP Header	163
The TCP Three-Way Handshake	166
The First Shake: The SYN Packet	166
The Second Shake: The SYN/ACK Packet	168
The Third Shake: The ACK Packet	168
After the Shaking	169
TCP Summary	169
User Datagram Protocol (UDP)	170
UDP Error Messages	172
Internet Control Message Protocol (ICMP)	172
ICMP Header	173
ICMP Packet Structure	173
ICMP Common Examples	176
Risks and Vulnerabilities Associated with IP Protocols	178
Common Threats	178
CIA Triad	180

PPPN	184
Process	184
Physical	184
Platform	185
Network	186
Threats	186
Malicious Hackers	186
Attacking Methodology	187
Malicious Code	189
Virus	189
Worms	189
Trojan Horses	190
Logic Bomb	190
Denial-of-Service Attacks	190
Distributed Denial-of-Service Attacks	191
Social Engineering	191
Attacks Against Access Control Systems	193
Man-in-the-Middle (MITM)	193
Threats Summary	194
Controls	194
Access Control	195
Mandatory Access Control	195
Discretionary Access Control	196
Lattice-Based Access Control	197
Rule-Based Access Control	198
Role-Based Access Control	198
Access Control Lists	198
Single Sign-On	201
Script-Based Single Sign-On	201
Host-Based Single Sign-On	201
Access Control Methods	202
One-Time Passwords	202
Password Selection	203
Access Control Goals	203
Two-Factor Authentication	203
RADIUS	204
802.1x	204
The Role of RADIUS in 802.1x	205
TACACS	205
Access Control Zone of Control	206
Firewalls	206
Types of Firewalls	206
Caching	214
Proxy Firewall Recap	214
Network Segmentation/Subdomain Isolation	215
Virtual Local Area Networks (VLANs)	215
Physical Distance	215

Subnetting for Isolation	216
Routing for Isolation	218
Firewall for Isolation	218
Intrusion Detection Systems	218
Types of Intrusions	219
Network- Versus Host-Based Intrusion Detection Systems	219
IDS Information Processing	220
IDS Versus IPS	222
Cryptography	222
Goals of Cryptography	224
Nonrepudiation	224
Cryptographic Definitions	225
Kerckhoff's Principle	226
Private or Secret Key Cryptography	227
The Advanced Encryption Standard	230
Public Key Cryptography	231
Stream Ciphers	233
Block Ciphers	235
The Initialization Vector	235
Methods of Attack	237
One-Way Functions	238
Digital Signatures	239
Classic Cryptographic Systems	240
Substitution Ciphers	240
Transposition Ciphers	241
Poly-Alphabetic Cipher	242
Running Key Cipher	242
Concealment	243
Steganography	243
Codes	244
Encryption Machines	244
Secure Sockets Layer (SSL)	245
Message Authentication Codes	248
Public Key Infrastructure	248
Certificate Authority (CA)	249
Registration Authority (RA)	249
Certificate Repository	249
Certificate Revocation System	249
IPSEC	249
Project Management for Information Security Managers	250
Baselines	251
Wireless	252
How It Works	253
The Alphabet Soup	254
Securing Wireless—The Early Days	254
RC4 and the One-Time Pad	255
WEP's Implementation of RC4	256

Weakness: Key Management and Key Size	257
Help! My IV Is Too Small	258
The ICV and Its Weakness	258
RC4	259
The Problems With Message Authentication	259
Another Standard 802.1x	260
The 802.1x Function	261
The Relationship between EAP and 802.1x	261
More on 802.1x	263
802.1x Doesn't Work Alone	266
802.1x – Making Wireless Better	266
802.1x's Partner TKIP	266
Back to the Alphabet Soup One Last Time—802.11i	268
Wireless Summary	268
Buffer Overflows versus Application Security	269
Virtual Private Networks (VPNs)	270
Web Server Security versus Internet Security	270
Security Testing	271
Vulnerability Assessment	272
Vulnerability Assessment	272
Penetration Testing	273
Risk Assessment	273
Hybrid Approach to Security Testing	273
Summary	273
What Was Covered in This Chapter	274
Questions	275

4 Information Security Management.....293

Functional Area Overview	293
CISM Mapping	295
Introduction	295
Information Systems Compliance	297
Administrative Procedures	298
Ensure Services Outsourced Are Consistent	305
Measure, Monitor, and Report Effectiveness and Efficiency of the Controls and Compliance Policies	307
Ensure That Information Security Is Not Compromised Throughout the Change Management Process	309
Perform Vulnerability Assessments to Evaluate Effectiveness of Existing Controls	311
Ensure That Noncompliance Issues and Other Variances Are Resolved in a Timely Manner	318
Information Security Awareness and Education	322
Introduction	322
Key Security Requirements	323
Believe in What You Are Doing	324

Program Goals.....	326
Segmenting the Audience.....	328
Current Level of Computer Usage.....	328
What Does the Audience Really Want to Learn?	328
Determine How Receptive the Audience Is	329
Seek Out Ways to Gain Acceptance	329
Possible Allies.....	330
Program Development.....	331
Methods to Convey the Message.....	332
Presentation Keys.....	334
Presentation Format	336
Effective Communication.....	336
When to Do Awareness	338
Presentation Styles	339
Senior Management.....	339
Managers.....	340
Line Supervisors and Employees	340
The Message.....	340
Summary	341
What Was Covered in This Chapter.....	341
Questions.....	342

5 Response Management351

Functional Area Overview.....	351
CISM Mapping.....	351
Introduction.....	352
Threat Source Information	352
The Role of Intrusion Detection and Anti-Virus Systems.....	354
IDS Properties.....	354
Business Continuity Planning and Disaster Recovery Planning	355
The Planning	356
Business Continuity Planning and Disaster Recovery Planning	356
BCP Resources.....	358
Stages of BCP	358
Reasons for BCP.....	358
BCP Responsibilities.....	360
Types of Plans.....	360
Business Continuity Plan (BCP).....	360
Business Recovery Plan (BRP), also Business Resumption Plan	361
Continuity of Operations Plan (COOP)	362
Continuity of Support Plan/IT Contingency Plan/Network	
Contingency Plan	362
Crisis Communications Plan.....	362
Cyber Incident Response Plan.....	363
Disaster Recovery Plan (DRP).....	363
Occupant Emergency Plan (OEP)	363

Business Impact Analysis (BIA).....	363
Performing a BIA	365
Business Impact Analysis Results.....	368
Reasons for BIA	368
Finding Resources and Dependencies	369
Alternate Sites.....	370
Cold Sites	372
Warm Sites	372
Hot Sites.....	372
Mobile Sites	372
Mirrored Sites.....	373
Reciprocal Agreements	373
Implementation and Writing	374
Team Training.....	374
Testing the Plan	375
Exercising and Testing the BCP/DRP	375
Improve the Plan	376
Updating the Plan	377
Three Phases of BCP	377
Incident Response.....	379
Discovery	380
Notification.....	380
Preliminary Investigation	382
Goals of the Investigation	382
Disclosure	383
Conducting Surveillance	383
Electronic Surveillance.....	384
Physical Surveillance.....	384
Running the Investigation	386
Factors of Investigation	387
Most Likely Suspects—Insiders, Outsiders, and Collaboration	388
Suspects/Witnesses/Interview	389
Freezing the Environment	390
Team Members.....	390
Post-Incident Access	391
Seizing the System	391
Forensic Processes	393
Inventory Internal Devices.....	395
Forensic Processing—Imaging	396
Live System Variation.....	400
Forensic Processing—Imaging	401
Forensic Reporting	403
Criminal and Civil Courts	403
Types of Evidence	403
Exclusionary Rule.....	404
Evidence Life Cycle.....	404
Incident Post Mortems	404

Incident Response Training.....	405
Difficulties with Following the Plan.....	406
Containment.....	407
Government Facilities to Assist in Planning for a Disaster.....	408
Escalation Procedures and Notification.....	408
Help Desk Training.....	408
Summary.....	409
What Was Covered in This Chapter.....	409
Questions.....	410
Index.....	429