

Table of Contents

INTRODUCTION	xxvii
LAB REQUIREMENTS	xxxv
CHAPTER 1	
Information Security and Risk Management	1
Organizational Purpose	2
Mission	3
Objectives	3
Goals	3
Security Support of Mission, Objectives, and Goals	4
Risk Management	4
Risk Management Principles	4
Risk Assessment	4
Qualitative Risk Assessment	4
Quantitative Risk Assessment	5
Quantifying Countermeasures	6
Geographic Considerations	7
Specific Risk Assessment Methodologies	7
Risk Treatment	8
Risk Avoidance	8
Risk Mitigation	8
Risk Acceptance	8
Risk Transfer	8
Residual Risk	8
Security Management Concepts	8
Security Controls	9
The CIA Triad	9
Confidentiality	9
Integrity	10
Availability	10
Defense in Depth	10
Single Points of Failure	11
Fail Open, Fail Closed, Fail Soft	12
Privacy	12
Personally Identifiable Information	12
Security Management	13
Security Executive Oversight	13
Security Governance	13
Security Policies, Requirements, Guidelines, Standards, and Procedures	14
Policies	14
Policy Standards	14
Policy Effectiveness	15
Requirements	15
Guidelines	16
Standards	16
Procedures	16
Security Roles and Responsibilities	17

Service Level Agreements	17
Secure Outsourcing	17
Data Classification and Protection	18
Sensitivity Levels	19
Information Labeling	19
Handling	20
Destruction	21
Certification and Accreditation	21
Internal Audit	21
Security Strategies.....	22
Personnel Security	22
Hiring Practices and Procedures.....	22
Non-Disclosure Agreement	23
Background Verification	23
Offer Letter	24
Non-Compete Agreement	24
Intellectual Property Agreement.....	24
Employment Agreement	24
Employee Handbook	24
Formal Job Descriptions	24
Termination.....	25
Work Practices.....	25
Separation of Duties.....	25
Job Rotation	26
Mandatory Vacations.....	26
Security Education, Training, and Awareness	26
Chapter Summary	27
Key Terms.....	28
Review Questions.....	31
Hands-On Projects	33
Case Projects	35
CHAPTER 2	
Access Controls	37
Controlling Access to Information and Functions	38
Identification and Authentication.....	39
Authentication Methods	39
How Information Systems Authenticate Users.....	40
How a User Should Treat Userids and Passwords	41
How a System Stores Userids and Passwords	41
Possession-Based Authentication	41
Biometric Authentication.....	43
Multi-Factor Authentication	44
Authentication Issues	45
Access Control Technologies and Methods.....	45
Single Sign-On	45
Reduced Sign-On	46
LDAP	46
Active Directory.....	46

RADIUS	46
Diameter	47
TACACS	47
Kerberos	47
Access Control Attacks	48
Buffer Overflow	49
Script Injection	49
Data Remanence	50
Denial of Service	50
Dumpster Diving	50
Eavesdropping	51
Emanations	51
Spoofing and Masquerading	52
Social Engineering	52
Phishing	53
Pharming	54
Password Guessing	55
Password Cracking	55
Rainbow Tables	55
Malicious Code	56
Access Control Processes	57
Access Requests and Provisioning	57
Personnel Internal Transfers	58
Personnel Termination	58
Periodic Access Review	58
Internal and External Audit	58
Access Control Concepts	59
Principles of Access Control	59
Separation of Duties	59
Least Privilege	60
Least Privilege and Server Applications	60
User Permissions on File Servers and Applications	60
Least Privilege on Workstations	60
Types of Controls	61
Technical Controls	61
Physical Controls	61
Administrative Controls	62
Categories of Controls	62
Detective Controls	62
Deterrent Controls	63
Preventive Controls	64
Corrective Controls	64
Recovery Controls	65
Compensating Controls	65
Using a Defense in Depth Controls Strategy	65
Example 1: Protected Application	66
Example 2: Protected Facility	67
Testing Access Controls	67
Vulnerability Scanning	67
Penetration Testing	68

Application Vulnerability Testing.....	68
Audit Log Analysis.....	69
Chapter Summary	70
Key Terms.....	71
Review Questions.....	74
Hands-On Projects.....	76
Case Projects	84
 CHAPTER 3	
Software Development Security.....	87
Operating Systems	88
Operating System Components	88
Operating System Security Functions.....	89
Threats to Operating Systems	89
Applications.....	89
Agents.....	90
Applets	90
Client-Server Applications.....	90
Distributed Applications.....	93
Thin Client Web Applications.....	93
Software Models and Technologies	95
Control Flow Languages.....	95
Structured Languages	95
Object-Oriented Systems.....	96
Object-Oriented Programming.....	96
Class.....	96
Object.....	96
Method.....	96
Encapsulation	96
Inheritance.....	96
Polymorphism	96
Distributed Object-Oriented Systems	97
Knowledge-Based Systems.....	97
Neural Networks	97
Expert Systems.....	97
Threats in the Software Environment.....	97
Software Attack Approaches.....	98
Buffer Overflow.....	98
Types of Buffer Overflow Attacks	99
Stack Buffer Overflow	99
NOP Sled Attack	99
Heap Overflow	99
Jump-to-Register Attack	99
Historic Buffer Overflow Attacks.....	99
Buffer Overflow Countermeasures.....	100
Malicious Software.....	101
Components of Malicious Software	101
Types of Malicious Software	102

Viruses	102
Worms	103
Trojan Horses	104
Rootkits	104
Bots	105
Remote Access Trojans (RATs)	105
Spam.	105
Pharming.	106
Spyware and Adware	106
Malicious Software Countermeasures.	107
Anti-Virus	108
Anti-Rootkit Software.	108
Anti-Spyware Software	108
Anti-Spam Software	109
Firewalls	109
Decreased Privilege Levels.	111
Application Whitelisting	111
Process Profiling.	111
Penetration Testing.	111
Hardening	112
Input Attacks.	112
Types of Input Attacks	113
Input Attack Countermeasures	113
Object Reuse	114
Object Reuse Countermeasures	114
Mobile Code	114
Mobile Code Countermeasures	114
Social Engineering	115
Social Engineering Countermeasures	115
Back Door.	115
Back Door Countermeasures	116
Logic Bomb.	116
Logic Bomb Countermeasures	116
Security in the Software Development Life Cycle.	116
Security in the Conceptual Stage	117
Security Application Requirements and Specifications	117
Security in Application Design.	118
Threat Risk Modeling.	119
Security in Application Coding	119
Common Vulnerabilities to Avoid	119
Use Safe Libraries.	120
Security in Testing	120
Protecting the SDLC Itself.	120
Application Environment and Security Controls	121
Authentication	122
Authorization.	122
Role-Based Access Control	122
Audit Log	122
Audit Log Contents	123
Audit Log Protection	123

Databases and Data Warehouses	123
Database Concepts and Design	123
Database Architectures	124
Relational Databases	124
Object-Oriented Databases	124
Distributed Databases	124
Hierarchical Databases	124
Network Databases	125
NoSQL Databases	125
Database Transactions	125
Database Security Controls	126
Access Controls	126
Views	126
Chapter Summary	126
Key Terms	127
Review Questions	131
Hands-On Projects	133
Case Projects	137
 CHAPTER 4	
Business Continuity and Disaster Recovery Planning	139
Business Continuity and Disaster Recovery Planning Basics	140
What Is a Disaster?	140
Natural Disasters	140
Man-Made Disasters	141
How Disasters Affect Businesses	141
Direct Damage	141
Casualties	141
Transportation	141
Communications	142
Utilities	142
How BCP and DRP Support Data Security	143
BCP and DRP Differences and Similarities	143
Industry Standards	143
Benefits of BC and DR Planning	144
The Role of Prevention	145
Competitive Advantage	145
The BCP and DRP Life Cycle	145
Running a BCP/DRP Project	145
Pre-Project Activities	145
Obtaining Executive Support	146
Defining the Project Scope	146
Choosing Project Team Members	147
Developing a Project Plan	147
Developing a Project Charter	148
Business Impact Analysis	148
Survey In-Scope Business Processes	149
Information Collection	149
Information Consolidation	149

Threat and Risk Analysis	149
Threat Analysis	151
Risk Analysis	151
Determine Maximum Tolerable Downtime (MTD)	151
Develop Statements of Impact	152
Recording Other Key Metrics	152
Develop Current Continuity and Recovery Capabilities	152
Developing Key Recovery Targets	152
Recovery Time Objective (RTO)	153
Recovery Point Objective (RPO)	153
Recovery Consistency Objective (RCO)	154
Recovery Capacity Objective (RCapO)	154
Establishing Ranking Criteria	155
Complete the Criticality Analysis	155
Improving System and Process Resilience	155
Identifying Risk Factors	155
Developing Business Continuity and Disaster Recovery Plans	155
Selecting Recovery Team Members	156
Emergency Response	157
Damage Assessment and Salvage	157
Notification	157
Personnel Safety	158
Communications	159
Public Utilities and Infrastructure	159
Electricity	159
Water	160
Natural Gas	160
Wastewater Treatment	160
Steam	160
Logistics and Supplies	160
Fire Protection	161
Business Resumption Planning	161
Restoration and Recovery	162
Improving System Resilience and Recovery	162
Off-Site Media Storage	163
Server Clusters	163
Data Replication	164
Training Staff on Business Continuity and Disaster Recovery Procedures	164
Testing Business Continuity and Disaster Recovery Plans	165
Document Review	165
Walkthrough	165
Simulation	165
Parallel Test	165
Cutover Test	166
Maintaining Business Continuity and Disaster Recovery Plans	166
Chapter Summary	167
Key Terms	168
Review Questions	170
Hands-On Projects	172
Case Projects	173

CHAPTER 5	
Cryptography	175
Applications and Uses of Cryptography	176
Encryption Terms and Operations	177
Plaintext	177
Ciphertext	177
Encryption	177
Decryption	177
Encryption Key	177
Encryption Methodologies	178
Methods of Encryption	178
Substitution	178
Transposition	179
Monoalphabetic	179
Polyalphabetic	179
Running Key Cipher	180
One-Time Pads	180
Types of Encryption	181
Block Ciphers	181
Block Cipher Modes of Operation	181
Electronic Codebook (ECB)	182
Cipher-Block Chaining (CBC)	182
Cipher Feedback (CFB)	182
Output Feedback (OFB)	183
Counter (CTR)	183
Stream Ciphers	183
Types of Encryption Keys	185
Symmetric Keys	185
Asymmetric Key Cryptography	185
Key Exchange Protocols	186
Diffie-Hellman Key Exchange	187
Length of Encryption Keys	188
Protection of Encryption Keys	188
Protecting Symmetric Keys	189
Protecting Public Cryptography Keys	189
Protecting Encryption Keys Used by Applications	189
Cryptanalysis—Attacks on Cryptosystems	190
Frequency Analysis	190
Birthday Attacks	190
Ciphertext-Only Attack	190
Chosen Plaintext Attack	190
Chosen Ciphertext Attack	191
Known Plaintext Attack	191
Man in the Middle Attack	191
Replay Attack	191
Rubber Hose Attack	191
Social Engineering Attack	191
Application and Management of Cryptography	191
Uses for Cryptography	192
File Encryption	192
Disk Encryption	192

E-Mail Security	193
Secure/Multipurpose Internet Mail Extensions (S/MIME).....	193
PGP	193
PEM.....	193
MOSS.....	193
Secure Point-to-Point Communications.....	193
SSH	193
IPsec.....	193
SSL and TLS	194
Web Browser and e-Commerce Security.....	194
Web Services Security.....	194
Secure Hypertext Transfer Protocol (S-HTTP)	195
Secure Electronic Transaction (SET).....	195
Cookies: Used for Session and Identity Management.....	195
Virtual Private Networks	196
Key Management	196
Key Creation	197
Key Protection and Custody	197
Key Rotation	197
Key Destruction	197
Key Escrow	198
Message Digests and Hashing	198
Digital Signatures	199
Digital Certificates	199
Non-Repudiation	200
Public Key Infrastructure (PKI)	200
Encryption Alternatives.....	201
Steganography	201
Watermarking	201
Trusting Cryptography	202
Chapter Summary	202
Key Terms	203
Review Questions.....	207
Hands-On Projects	209
Case Projects	216
 CHAPTER 6	
Legal, Regulations, Investigations, and Compliance	219
Computers and Crime	220
The Role of Computers in Crime.....	220
The Trend of Increased Threats in Computer Crimes	221
Categories of Computer Crimes.....	222
Espionage and Cyber-warfare	223
Terrorism	223
Theft and Fraud.....	223
Commercial Espionage	224
Harassment	225
Hacktivism	225
Cybervandalism	225

Computer Crime Laws and Regulations	225
Categories of U.S. Laws	225
U.S. Computer Crime Laws	226
U.S. Intellectual Property Law	226
U.S. Privacy Law	227
U.S. Computer Crime Law	228
Canadian Computer Crime Laws	229
European Computer Crime Laws	230
Computer Crime Laws in Other Countries	231
Managing Compliance	231
Security Incident Response	233
The Security Incident Response Process	233
Incident Declaration	233
Triage	234
Investigation	234
Analysis	234
Containment	234
Recovery	235
Debriefing	235
Continuous Improvement	236
Assumption of Breach	236
Incident Management Preventive Measures	236
Incident Response Training, Testing, and Maintenance	237
Incident Response Process Models	237
Reporting Incidents to Management	238
Investigations	238
Working with Law Enforcement Authorities	239
Forensic Techniques and Procedures	239
Identifying and Gathering Evidence	240
Evidence Collection Techniques	240
Preserving Evidence	241
Chain of Custody	242
Presentation of Findings	242
Ethical Issues	242
Professional Ethics	243
Codes of Conduct	243
RFC 1087: Ethics and the Internet	244
The (ISC) ² Code of Ethics	244
Guidance on Ethical Behavior	245
Chapter Summary	246
Key Terms	247
Review Questions	249
Hands-On Projects	251
Case Projects	253
CHAPTER 7	
Security Operations	255
Security Operations Concepts	257
Need-to-Know	257

Least Privilege	258
Separation of Duties	258
Job Rotation	259
Monitoring of Special Privileges.	260
Records Management Controls	260
Data Classification	261
Access Management	261
Record Retention	262
Backups	263
Data Restoration	263
Protection of Backup Media	263
Offsite Storage of Backup Media	264
Data Destruction	264
Anti-Malware	265
Applying Defense-In-Depth Malware Protection	265
Central Anti-Malware Management	266
Remote Access	266
Risks and Remote Access	266
Administrative Management and Control	268
Types and Categories of Controls	269
Employing Resource Protection	269
Facilities	270
Hardware	270
Software	272
Documentation	272
Incident Management	273
High-Availability Architectures	273
Fault Tolerance	274
Clusters	275
Failover	275
Replication	275
Virtualization.	276
Business Continuity Management	276
Vulnerability Management	277
Vulnerability Scanning	277
Application Scanning	277
Penetration Testing.	278
Source Code Reviews and Scanning.	278
Threat Modeling	278
Patch Management.	278
Change Management	279
Configuration Management.	280
Operations Attacks and Countermeasures	280
Social Engineering	280
Sabotage	280
Theft and Disappearance	281
Extortion.	281
Bypass.	281
Denial of Service	281

Chapter Summary	282
Key Terms	284
Review Questions.....	286
Hands-On Projects	289
Case Projects	290
CHAPTER 8	
Physical and Environmental Security	293
Site Access Security	294
Site Access Control Strategy	294
Site Access Controls	295
Key Cards	296
Biometric Access Controls.....	299
Metal Keys	300
Mantraps.....	300
Security Guards	300
Guard Dogs.....	301
Access Logs	301
Fences and Walls	302
Video Surveillance	302
Camera Types	302
Recording Capabilities	304
Intrusion, Motion, and Alarm Systems.....	304
Duress Alarms	305
Visible Notices.....	305
Exterior Lighting	305
Other Physical Controls	306
Security for Business Travelers	306
Personnel Privacy	308
Secure Siting	308
Natural Threats	309
Man-Made Threats	310
Other Siting Factors	311
Equipment Protection	311
Theft Protection	311
Damage Protection	312
Fire Protection	313
Fire Extinguishers.....	313
Smoke Detectors	313
Fire Alarm Systems.....	314
Automatic Sprinkler Systems.....	314
Gaseous Fire Suppression	315
Cabling Security.....	316
Environmental Controls	317
Heating and Air Conditioning.....	317
Humidity.....	317
Electric Power	318
Line Conditioner	318
Uninterruptible Power Supply (UPS).....	318

Electric Generator	319
Redundant Controls.....	319
Chapter Summary	320
Key Terms.....	322
Review Questions.....	324
Hands-On Projects	326
Case Projects	328
 CHAPTER 9	
Security Architecture and Design.....	329
Security Concepts.....	330
Security Models	331
Bell-LaPadula.....	332
Biba	332
Clark-Wilson.....	332
Access Matrix	333
Multilevel	333
Mandatory Access Control (MAC)	334
Discretionary Access Control (DAC)	334
Role-Based Access Control (RBAC).....	334
Rule-Based Access Control	334
Non-Interference	335
Information Flow.....	335
Information Systems Evaluation Models.....	335
Common Criteria.....	335
TCSEC	336
Trusted Network Interpretation (TNI).....	337
ITSEC	337
SEI-CMMI.....	338
SSE-CMM.....	338
Certification and Accreditation	338
FedRAMP	339
FISMA	339
DITSCAP	339
DIACAP	340
NIACAP	340
DCID 6/3	340
Computer Hardware Architecture	341
Central Processor	341
Components	341
Operations.....	341
Instruction Sets	342
Single-Core and Multi-Core Designs	343
Single- and Multi-Processor Computers	343
CPU Security Features	343
Bus	343
Storage	345
Main Storage.....	345
Secondary Storage	346

Virtual Memory	346
Swapping	346
Paging	347
Communications	347
Firmware	347
Trusted Computing Base (TCB)	348
Reference Monitor	348
Virtualization	348
Security Hardware	348
Trusted Platform Module	349
Hardware Authentication	349
Security Modes	349
Security Countermeasure Principles	350
Defense in Depth	350
System Hardening	351
Attack Surface	351
Security through Obfuscation	351
Single Use	352
Homogeneous and Heterogeneous Environments	352
Software	352
Operating Systems	353
Subsystems	353
Programs, Tools, and Applications	354
Software Security Threats	355
Covert Channels	355
Side-Channel Attacks	356
Inference Attacks	356
Aggregation Attack	356
State Attacks (TOCTTOU)	356
Emanations	357
Maintenance Hooks and Back Doors	357
Privileged Programs	357
Supply Chain Attacks	357
Software Security Countermeasures	358
Sniffers and Other Analyzers	358
Source Code Reviews	358
Auditing Tools	359
Vulnerability Scanning Tools	359
Penetration Testing	359
Cloud Computing Threats and Countermeasures	360
Multitenancy and Logical Separation	360
Data Sovereignty	360
Data Jurisdiction	361
Controls and Audits	361
Chapter Summary	362
Key Terms	364
Review Questions	369
Hands-On Projects	372
Case Projects	374

CHAPTER 10	
Telecommunications and Network Security	375
Telecommunications Technologies	376
Wired Telecom Technologies	376
DS-1	376
SONET	377
MPLS	377
DSL	378
ATM	378
Other Wireline Technologies	378
Wireless Telecom Technologies	380
CDMA2000	380
GPRS	380
EDGE	380
LTE	380
UMTS	380
WiMAX	380
Other Wireless Telecom Technologies	381
Network Technologies	381
Wired Network Technologies	381
Ethernet	381
Ethernet Cable Types	381
Ethernet Frame Layout	382
Ethernet Error Detection	383
Ethernet MAC Addressing	383
Ethernet Devices	383
Token Ring	384
USB	384
RS-232	385
Network Cable Types	386
Network Topologies	387
Wireless Network Technologies	387
WiFi	388
WiFi Standards	388
WiFi Security	388
Bluetooth	389
IrDA	389
Wireless USB	389
Near Field Communication	389
Network Protocols	390
The OSI Network Model	390
Physical	390
Data Link	390
Network	391
Transport	392
Session	392
Presentation	392
Application	392
TCP/IP	392
TCP/IP Link Layer	393
TCP/IP Internet Layer	394

Internet Layer Protocols	394
Internet Layer Routing Protocols	395
Internet Layer Addressing	395
TCP/IP Transport Layer	397
TCP Transport Protocol	397
UDP Transport Protocol	398
TCP/IP Application Layer	398
TCP/IP Routing Protocols	399
RIP	400
IGRP	400
EIGRP	400
OSPF	400
IS-IS	400
BGP	400
Remote Access/Tunneling Protocols	401
VPN	401
SSL/TLS	402
SSH	402
IPsec	402
L2TP	402
PPTP	402
PPP	402
SLIP	403
Network Authentication Protocols	403
RADIUS	403
Diameter	403
TACACS	403
802.1X	403
NAC	403
CHAP	404
EAP	404
PEAP	405
PAP	405
Network-Based Threats, Attacks, and Vulnerabilities	405
Threats	405
Attacks	405
DoS	405
DDoS	406
Teardrop	406
Sequence Number	406
Smurf	406
Ping of Death	407
SYN Flood	407
Worms	407
Spam	407
Phishing	407
Vulnerabilities	407
Unnecessary Open Ports	408
Unpatched Systems	408
Poor and Outdated Configurations	409
Default Passwords	409
Exposed Cabling	409

Network Countermeasures	409
Access Control Lists	409
Firewalls	409
Intrusion Detection Systems (IDS)	410
Intrusion Prevention Systems (IPS)	410
Data Leakage Prevention Systems (DLP)	410
Network Cabling Protection	411
Anti-Virus Software	411
Private Addressing	411
Closure of Unnecessary Ports and Services	411
Security Patches	411
Unified Threat Management	411
Gateways.....	412
Chapter Summary	412
Key Terms.....	414
Review Questions.....	422
Hands-On Projects	424
Case Projects	431
APPENDIX A	
The Ten Domains of CISSP Security	433
Changes in the CBK.....	435
The Common Body of Knowledge.....	435
Domain 1: Access Control	435
Domain 2: Telecommunications and Network Security	436
Domain 3: Information Security Governance & Risk Management.....	436
Domain 4: Software Development Security.....	436
Domain 5: Cryptography	437
Domain 6: Security Architecture & Design.....	437
Domain 7: Security Operations	438
Domain 8: Business Continuity & Disaster Recovery Planning.....	438
Domain 9: Legal, Regulations, Investigations and Compliance	438
Domain 10: Physical (Environmental) Security	439
Key Terms.....	439
APPENDIX B	
The (ISC)² Code of Ethics	441
The (ISC) ² Code of Ethics.....	442
The Pursuit of Integrity, Honor, and Trust in Information Security.....	442
Code of Ethics Preamble:	442
Code of Ethics Canons:	442
Objectives for Guidance	442
Protect Society, the Commonwealth, and the Infrastructure	443
Act Honorably, Honestly, Justly, Responsibly, and Legally	443
Provide Diligent and Competent Service to Principals	443
Advance and Protect the Profession	443
An Ethical Challenge	444