



Contents

About the Authors	vii
Foreword	xxiii
Acknowledgments	xxv
Introduction	xxvii
Part 1 Focused Review of the CISSP Ten Domains	1
Chapter 1 Information Security and Risk Management	3
Our Approach	4
Security Management Concepts	5
System Security Life Cycle	5
The Three Fundamentals	6
Other Important Concepts	7
Objectives of Security Controls	10
Information Classification Process	12
Information Classification Objectives	12
Information Classification Benefits	13
Information Classification Concepts	13
Information Classification Roles	16
Security Policy Implementation	20
Policies, Standards, Guidelines, and Procedures	20
Roles and Responsibilities	25
Risk Management and Assessment	27
Principles of Risk Management	27
RM Roles	30
Overview of Risk Analysis	30
Security Posture Assessment Methodologies	39

Security Awareness	42
Awareness	44
Training and Education	45
Assessment Questions	46
Chapter 2 Access Control	55
Rationale	55
Controls	56
Models for Controlling Access	57
Control Combinations	59
Access Control Attacks	61
Denial of Service/Distributed Denial of Service (DoS/DDoS)	61
Back Door	62
Spoofing	62
Man-in-the-Middle	63
Replay	63
TCP Hijacking	63
Social Engineering	64
Dumpster Diving	64
Password Guessing	65
Software Exploitation	65
Mobile Code	66
Trojan Horses	66
Logic Bomb	67
System Scanning	67
Penetration Testing	68
Identification and Authentication	69
Passwords	70
Biometrics	72
Single Sign-On (SSO)	74
Kerberos	75
Kerberos Operation	76
SESAME	79
KryptoKnight	79
Access Control Methodologies	79
Centralized Access Control	80
Decentralized/Distributed Access Control	81
Intrusion Detection	86
Some Access Control Issues	88
Assessment Questions	89
Chapter 3 Telecommunications and Network Security	95
The C.I.A. Triad	96
Confidentiality	96
Integrity	96
Availability	97

Protocols	98
The Layered Architecture Concept	98
Open Systems Interconnect (OSI) Model	99
Transmission Control Protocol/Internet Protocol (TCP/IP)	103
LAN Technologies	110
Ethernet	110
ARCnet	112
Token Ring	112
Fiber Distributed Data Interface (FDDI)	113
Cabling Types	113
Coaxial Cable (Coax)	113
Twisted Pair	114
Fiber-Optic Cable	116
Cabling Vulnerabilities	116
Transmission Types	117
Network Topologies	118
Bus	118
Ring	118
Star	118
Tree	120
Mesh	120
LAN Transmission Protocols	121
Carrier-Sense Multiple Access (CSMA)	121
Polling	122
Token Passing	122
Unicast, Multicast, Broadcast	123
Networking Devices	123
Hubs and Repeaters	123
Bridges	124
Spanning Tree	125
Switches	125
Transparent Bridging	125
Routers	126
VLANs	129
Gateways	130
LAN Extenders	130
Firewall Types	130
Packet-Filtering Firewalls	131
Application-Level Firewalls	132
Circuit-Level Firewalls	133
Stateful Inspection Firewalls	133
Firewall Architectures	133
Packet-Filtering Routers	134
Screened-Host Firewalls	134
Dual-Homed Host Firewalls	134
Screened-Subnet Firewalls	135
SOCKS	137

Common Data Network Services	137
File Transfer Services	138
SFTP	139
SSH/SSH-2	139
TFTP	140
Data Network Types	140
Wide Area Networks	141
Internet	141
Intranet	142
Extranet	142
WAN Technologies	142
Dedicated Lines	142
T-carriers	143
WAN Switching	143
Circuit-Switched Networks	143
Packet-Switched Networks	144
Other WAN Protocols	146
Common WAN Devices	146
Network Address Translation (NAT)	147
Remote Access Technologies	149
Remote Access Types	149
Remote Access Security Methods	151
Virtual Private Networking (VPN)	151
RADIUS and TACACS	160
Network Availability	162
High Availability and Fault Tolerance	162
Wireless Technologies	164
IEEE Wireless Standards	164
Bluetooth	170
Wireless Application Protocol (WAP)	171
Wireless Security	174
Wireless Transport Layer Security Protocol	174
WEP Encryption	175
Wireless Vulnerabilities	175
Intrusion Detection and Response	183
Types of Intrusion Detection Systems	183
IDS Approaches	184
Honey Pots	186
Computer Incident Response Team	187
IDS and a Layered Security Approach	188
IDS and Switches	188
IDS Performance	190
Network Attacks and Abuses	190
Logon Abuse	190
Inappropriate System Use	190
Eavesdropping	191
Network Intrusion	191

Denial of Service (DoS) Attacks	192
Session Hijacking Attacks	192
Fragmentation Attacks	193
Dial-Up Attacks	193
Probing and Scanning	194
Vulnerability Scanning	194
Port Scanning	195
Issues with Vulnerability Scanning	201
Malicious Code	202
Viruses	202
Spyware	204
Trojan Horses	210
Remote Access Trojans (RATs)	211
Logic Bombs	212
Worms	212
Malicious Code Prevention	212
Web Security	214
Phishing	214
Browser Hijacking	214
SSL/TLS	215
S-HTTP	217
Instant Messaging Security	217
8.3 Naming Conventions	221
Assessment Questions	222
Chapter 4	
Cryptography	233
Introduction	233
Definitions	234
Background	238
Cryptographic Technologies	241
Classical Ciphers	241
Substitution	241
Transposition (Permutation)	244
Vernam Cipher (One-Time Pad)	244
Book or Running-Key Cipher	245
Codes	245
Steganography	245
Secret-Key Cryptography (Symmetric-Key)	246
Data Encryption Standard (DES)	247
Triple DES	251
The Advanced Encryption Standard (AES)	252
The Rijndael Block Cipher	253
The Twofish Algorithm	254
The IDEA Cipher	255
RC5/RC6	255
Public-Key (Asymmetric) Cryptosystems	255
One-Way Functions	256
Public-Key Algorithms	256

Public-Key Cryptosystem Algorithm Categories	260
Asymmetric and Symmetric Key Length Strength Comparisons	260
Digital Signatures	260
Digital Signature Standard (DSS) and Secure Hash Standard (SHS)	261
MD5	262
Sending a Message with a Digital Signature	263
Hashed Message Authentication Code (HMAC)	263
Hash Function Characteristics	264
Cryptographic Attacks	264
Public-Key Certification Systems	266
Digital Certificates	266
Public-Key Infrastructure (PKI)	267
Approaches to Escrowed Encryption	273
The Escrowed Encryption Standard	273
Key Escrow Approaches Using Public-Key Cryptography	275
Identity-Based Encryption	275
Cryptographic Export Issues	277
Quantum Computing	278
E-mail Security Issues and Approaches	279
Secure Multi-Purpose Internet Mail Extensions (S/MIME)	279
MIME Object Security Services (MOSS)	279
Privacy Enhanced Mail (PEM)	279
Pretty Good Privacy (PGP)	280
Internet Security Applications	281
Message Authentication Code (MAC) or the Financial Institution Message Authentication Standard (FIMAS)	281
Secure Electronic Transaction (SET)	281
Secure Sockets Layer (SSL)/Transaction Layer Security (TLS)	281
Internet Open Trading Protocol (IOTP)	282
MONDEX	282
IPSec	282
Secure Hypertext Transfer Protocol (S-HTTP)	283
Secure Shell (SSH-2)	284
Wireless Security	284
Wireless Application Protocol (WAP)	284
The IEEE 802.11 Wireless Standard	286
Assessment Questions	289
Chapter 5 Security Architecture and Design	297
Computer Architecture	298
Memory	299
Instruction Execution Cycle	302
Input/Output Structures	304
Software	305
Open and Closed Systems	307
Distributed Architecture	307

Protection Mechanisms	309
Rings	310
Logical Security Guard	311
Enterprise Architecture Issues	311
Security Labels	312
Security Modes	312
Additional Security Considerations	313
Recovery Procedures	314
Assurance	314
Evaluation Criteria	315
Certification and Accreditation	317
DITSCAP and NIACAP	317
The Systems Security Engineering Capability Maturity Model (SSE-CMM)	319
Information Security Models	322
Access Control Models	322
Integrity Models	327
Information Flow Models	329
Assessment Questions	332
Chapter 6 Operations Security	339
Operations Security Concepts	340
Triples	340
C.I.A.	340
Controls and Protections	341
Categories of Controls	341
Orange Book Controls	342
Operations Controls	358
Monitoring and Auditing	365
Monitoring	365
Auditing	369
Threats and Vulnerabilities	373
Threats	373
Vulnerabilities and Attacks	375
Maintaining Resource Availability	376
RAID	376
RAID Levels	377
Backup Concepts	378
Operational E-Mail Security	382
E-Mail Phishing	383
Fax Security	387
Assessment Questions	388
Chapter 7 Application Security	397
Systems Engineering	398
The System Life Cycle or System Development Life Cycle (SDLC)	398

The Software Life Cycle Development Process	399
The Waterfall Model	400
The Spiral Model	403
Cost Estimation Models	406
Information Security and the Life Cycle Model	407
Testing Issues	408
The Software Maintenance Phase and the Change Control Process	408
Configuration Management	409
The Software Capability Maturity Model (CMM)	410
Agile Methodology	412
Object-Oriented Systems	413
Artificial Intelligence Systems	417
Expert Systems	417
Neural Networks	419
Genetic Algorithms	421
Knowledge Management	421
Database Systems	421
Database Security Issues	422
Data Warehouse and Data Mining	422
Data Dictionaries	423
Application Controls	423
Distributed Systems	425
Centralized Architecture	426
Real-Time Systems	426
Assessment Questions	427
Chapter 8 Business Continuity Planning and Disaster Recovery Planning	433
Business Continuity Planning	435
Continuity Disruptive Events	436
The Four Prime Elements of BCP	437
Disaster Recovery Planning (DRP)	446
Goals and Objectives of DRP	446
The Disaster Recovery Planning Process	447
Testing the Disaster Recovery Plan	455
Disaster Recovery Procedures	459
Other Recovery Issues	461
Assessment Questions	464
Chapter 9 Legal, Regulations, Compliance, and Investigations	473
Types of Computer Crime	473
Examples of Computer Crime	475
Law	477
Example: The United States	477
Common Law System Categories	478
Computer Security, Privacy, and Crime Laws	489

Investigation	496
Computer Investigation Issues	496
Export Issues and Technology	502
Liability	502
Ethics	504
(ISC) ² Code of Ethics	506
The Computer Ethics Institute’s Ten Commandments of Computer Ethics	506
The Internet Architecture Board (IAB) Ethics and the Internet (RFC 1087)	507
The U.S. Department of Health and Human Services Code of Fair Information Practices	507
The Organization for Economic Cooperation and Development (OECD)	508
Assessment Questions	510
Chapter 10 Physical (Environmental) Security	517
Threats to Physical Security	518
Controls for Physical Security	520
Administrative Controls	520
Environmental and Life Safety Controls	524
Physical and Technical Controls	534
Assessment Questions	550
Part 2 The Certification and Accreditation Professional (CAP) Credential	557
Chapter 11 Understanding Certification and Accreditation	559
System Authorization	559
A Select History of Systems Authorization	560
More and More Standards	572
What Is Certification and Accreditation?	572
NIST C&A Documents	573
C&A Roles and Responsibilities	573
C&A Phases	577
DIACAP Phases	578
Assessment Questions	580
Chapter 12 Initiation of the System Authorization Process	585
Security Categorization	586
Identification of Information Types	588
Potential Harmful Impact Levels	589
Assignment of Impact Level Scores	590
Assignment of System Impact Level	592
Initial Risk Estimation	593
Threat-Source Identification	594
Threat Likelihood of Occurrence	597
Analyzing for Vulnerabilities	597
System Accreditation Boundary	601
Legal and Regulatory Requirements	603

Selection of Security Controls	603
The Control Section	606
The Supplemental Guidance Section	606
The Control Enhancements Section	606
Assurance	607
Common and System-Specific Security Controls	608
Security Controls and the Management of Organizational Risk	608
Documenting Security Controls in the System Security Plan	610
Assessment Questions	613
Chapter 13 The Certification Phase	621
Security Control Assessment	622
Prepare for the Assessment	622
Conduct the Security Assessment	624
Prepare the Security Assessment Report	624
Security Certification Documentation	625
Provide the Findings and Recommendations	625
Update the System Security Plan	625
Prepare the Plan of Action	626
Assemble the Accreditation Package	626
DITSCAP Certification Phases	627
Phase 1: Definition	627
The System Security Authorization Agreement (SSAA)	630
SSAA Outline	630
SSAA Additional Material	632
The Requirements Traceability Matrix (RTM)	633
Phase 2: Verification	635
Key DITSCAP Roles	638
DIACAP Certification Phases	639
End of the Certification Phase	640
Assessment Questions	641
Chapter 14 The Accreditation Phase	645
Security Accreditation Decision	646
Final Risk Assessment	646
Accreditation Decision	647
Security Accreditation Documentation	648
Accreditation Package Transmission	648
System Security Plan Update	649
DITSCAP Accreditation Phases	649
Phase 3: Validation	649
Phase 4: Post Accreditation	653
DIACAP Accreditation Phases	656
End of the Accreditation Phase	657
Assessment Questions	658

Chapter 15	Continuous Monitoring Process	663
	Continuous Monitoring	664
	Monitoring Security Controls	665
	Configuration Management and Control	669
	Environment Monitoring	670
	Documentation and Reporting	671
	Assessment Questions	673
Appendix A	Answers to Assessment Questions	681
Appendix B	Glossary of Terms and Acronyms	881
Appendix C	The Information System Security Architecture Professional (ISSAP) Certification	945
Appendix D	The Information System Security Engineering Professional (ISSEP) Certification	951
Appendix E	The Information System Security Management Professional (ISSMP) Certification	1039
Appendix F	Security Control Catalog	1075
Appendix G	Control Baselines	1185
Index		1193

