

---

# CONTENTS AT A GLANCE

<b>Chapter 1</b>	Becoming a CISSP .....	1
<b>Chapter 2</b>	Security Trends .....	17
<b>Chapter 3</b>	Information Security and Risk Management .....	45
<b>Chapter 4</b>	Access Control .....	153
<b>Chapter 5</b>	Security Architecture and Design .....	281
<b>Chapter 6</b>	Physical and Environmental Security .....	401
<b>Chapter 7</b>	Telecommunications and Network Security .....	483
<b>Chapter 8</b>	Cryptography .....	665
<b>Chapter 9</b>	Business Continuity and Disaster Recovery .....	777
<b>Chapter 10</b>	Legal, Regulations, Compliance, and Investigations .....	845
<b>Chapter 11</b>	Application Security .....	921
<b>Chapter 12</b>	Operations Security .....	1049
<b>Appendix A</b>	Security Content Automation Protocol Overview .....	1133
<b>Appendix B</b>	About the CD-ROM .....	1141
	Glossary .....	1145
	Index .....	1161

---

# CONTENTS

	Forewords .....	xviii
	Acknowledgments .....	xxi
	Introduction .....	xxii
<b>Chapter 1</b>	<b>Becoming a CISSP .....</b>	<b>1</b>
	Why Become a CISSP? .....	1
	The CISSP Exam .....	2
	CISSP: A Brief History .....	7
	How Do You Become a CISSP? .....	8
	What Does This Book Cover? .....	8
	Tips for Taking the CISSP Exam .....	9
	How to Use This Book .....	11
	Questions .....	11
	Answers .....	15
<b>Chapter 2</b>	<b>Security Trends .....</b>	<b>17</b>
	How Security Became an Issue .....	17
	Areas of Security .....	20
	Benign to Scary .....	21
	Evidence of the Evolution of Hacking .....	22
	How Are Nations Affected? .....	25
	How Are Companies Affected? .....	27
	The U.S. Government's Actions .....	29
	Politics and Laws .....	33
	So What Does This Mean to Us? .....	35
	Hacking and Attacking .....	36
	Management .....	37
	A Layered Approach .....	39
	An Architectural View .....	40
	A Layer Missed .....	41
	Bringing the Layers Together .....	42
	Education .....	42
	Summary .....	43
<b>Chapter 3</b>	<b>Information Security and Risk Management .....</b>	<b>45</b>
	Security Management .....	45
	Security Management Responsibilities .....	46
	The Top-Down Approach to Security .....	47
	Security Administration and Supporting Controls .....	48
	Fundamental Principles of Security .....	51
	Availability .....	51
	Integrity .....	52
	Confidentiality .....	53
	Security Definitions .....	54
	Security Through Obscurity .....	56
	Organizational Security Model .....	57
	Security Program Components .....	59
	Information Risk Management .....	73
	Who Really Understands Risk Management? .....	73
	Information Risk Management Policy .....	74
	The Risk Management Team .....	75

Risk Analysis	76
The Risk Analysis Team	77
The Value of Information and Assets	78
Costs That Make Up the Value	79
Identifying Threats	80
Failure and Fault Analysis	83
Quantitative Risk Analysis	86
Qualitative Risk Analysis	91
Quantitative vs. Qualitative	94
Protection Mechanisms	95
Putting It Together	99
Total Risk vs. Residual Risk	100
Handling Risk	101
Policies, Standards, Baselines, Guidelines, and Procedures	102
Security Policy	103
Standards	106
Baselines	107
Guidelines	108
Procedures	108
Implementation	109
Information Classification	111
Private Business vs. Military Classifications	112
Classification Controls	115
Layers of Responsibility	117
Who's Involved?	117
The Data Owner	125
The Data Custodian	125
The System Owner	126
The Security Administrator	126
The Security Analyst	127
The Application Owner	127
The Supervisor	127
The Change Control Analyst	127
The Data Analyst	128
The Process Owner	128
The Solution Provider	128
The User	128
The Product Line Manager	129
The Auditor	129
Why So Many Roles?	129
Personnel	130
Structure	130
Hiring Practices	131
Employee Controls	133
Termination	133
Security-Awareness Training	134
Different Types of Security-Awareness Training	135
Evaluating the Program	136
Specialized Security Training	137
Summary	138
Quick Tips	139
Questions	142
Answers	148

<b>Chapter 4</b>	<b>Access Control</b> .....	<b>153</b>
	Access Controls Overview .....	153
	Security Principles .....	154
	Availability .....	155
	Integrity .....	155
	Confidentiality .....	155
	Identification, Authentication, Authorization, and Accountability .....	156
	Identification and Authentication .....	158
	Password Management .....	169
	Authorization .....	194
	Access Control Models .....	210
	Discretionary Access Control .....	210
	Mandatory Access Control .....	211
	Role-Based Access Control .....	213
	Access Control Techniques and Technologies .....	216
	Rule-Based Access Control .....	216
	Constrained User Interfaces .....	218
	Access Control Matrix .....	218
	Content-Dependent Access Control .....	220
	Context-Dependent Access Control .....	220
	Access Control Administration .....	221
	Centralized Access Control Administration .....	222
	Decentralized Access Control Administration .....	229
	Access Control Methods .....	229
	Access Control Layers .....	230
	Administrative Controls .....	230
	Physical Controls .....	232
	Technical Controls .....	233
	Access Control Types .....	236
	Preventive: Administrative .....	238
	Preventive: Physical .....	238
	Preventive: Technical .....	239
	Accountability .....	242
	Review of Audit Information .....	244
	Keystroke Monitoring .....	244
	Protecting Audit Data and Log Information .....	245
	Access Control Practices .....	245
	Unauthorized Disclosure of Information .....	246
	Access Control Monitoring .....	248
	Intrusion Detection .....	249
	Intrusion Prevention Systems .....	258
	A Few Threats to Access Control .....	260
	Dictionary Attack .....	261
	Brute Force Attacks .....	262
	Spoofing at Logon .....	262
	Summary .....	266
	Quick Tips .....	266
	Questions .....	269
	Answers .....	276
<b>Chapter 5</b>	<b>Security Architecture and Design</b> .....	<b>281</b>
	Computer Architecture .....	283
	The Central Processing Unit .....	283
	Multiprocessing .....	288

Operating System Architecture .....	289
Process Activity .....	296
Memory Management .....	297
Memory Types .....	300
Virtual Memory .....	308
CPU Modes and Protection Rings .....	309
Operating System Architecture .....	312
Domains .....	313
Layering and Data Hiding .....	314
The Evolution of Terminology .....	316
Virtual Machines .....	318
Additional Storage Devices .....	320
Input/Output Device Management .....	320
System Architecture .....	324
Defined Subsets of Subjects and Objects .....	325
Trusted Computing Base .....	326
Security Perimeter .....	329
Reference Monitor and Security Kernel .....	330
Security Policy .....	331
Least Privilege .....	332
Security Models .....	332
State Machine Models .....	334
The Bell-LaPadula Model .....	336
The Biba Model .....	338
The Clark-Wilson Model .....	341
The Information Flow Model .....	344
The Noninterference Model .....	347
The Lattice Model .....	348
The Brewer and Nash Model .....	350
The Graham-Denning Model .....	351
The Harrison-Ruzzo-Ullman Model .....	351
Security Modes of Operation .....	353
Dedicated Security Mode .....	353
System High-Security Mode .....	353
Compartmented Security Mode .....	354
Multilevel Security Mode .....	354
Trust and Assurance .....	356
Systems Evaluation Methods .....	357
Why Put a Product Through Evaluation? .....	357
The Orange Book .....	358
The Orange Book and the Rainbow Series .....	362
The Red Book .....	363
Information Technology Security Evaluation Criteria .....	364
Common Criteria .....	367
Certification vs. Accreditation .....	370
Certification .....	371
Accreditation .....	371
Open vs. Closed Systems .....	372
Open Systems .....	372
Closed Systems .....	373
Enterprise Architecture .....	373
A Few Threats to Review .....	382
Maintenance Hooks .....	382
Time-of-Check/Time-of-Use Attacks .....	383
Buffer Overflows .....	384
Summary .....	388

	Quick Tips .....	389
	Questions .....	392
	Answers .....	397
<b>Chapter 6</b>	<b>Physical and Environmental Security .....</b>	<b>401</b>
	Introduction to Physical Security .....	401
	The Planning Process .....	404
	Crime Prevention Through Environmental Design .....	408
	Designing a Physical Security Program .....	413
	Protecting Assets .....	428
	Internal Support Systems .....	429
	Electric Power .....	430
	Environmental Issues .....	434
	Ventilation .....	437
	Fire Prevention, Detection, and Suppression .....	438
	Perimeter Security .....	446
	Facility Access Control .....	447
	Personnel Access Controls .....	454
	External Boundary Protection Mechanisms .....	455
	Intrusion Detection Systems .....	464
	Patrol Force and Guards .....	468
	Dogs .....	468
	Auditing Physical Access .....	469
	Testing and Drills .....	469
	Summary .....	470
	Quick Tips .....	471
	Questions .....	473
	Answers .....	478
<b>Chapter 7</b>	<b>Telecommunications and Network Security .....</b>	<b>483</b>
	Open Systems Interconnection Reference Model .....	485
	Protocol .....	485
	Application Layer .....	489
	Presentation Layer .....	489
	Session Layer .....	491
	Transport Layer .....	492
	Network Layer .....	493
	Data Link Layer .....	494
	Physical Layer .....	496
	Functions and Protocols in the OSI Model .....	496
	Tying the Layers Together .....	498
	TCP/IP .....	499
	TCP .....	500
	IP Addressing .....	506
	IPv6 .....	508
	Types of Transmission .....	510
	Analog and Digital .....	510
	Asynchronous and Synchronous .....	511
	Broadband and Baseband .....	512
	LAN Networking .....	513
	Network Topology .....	513
	LAN Media Access Technologies .....	516
	Cabling .....	522
	Transmission Methods .....	528
	Media Access Technologies .....	529
	LAN Protocols .....	533

Routing Protocols .....	538
Networking Devices .....	541
Repeaters .....	541
Bridges .....	542
Routers .....	544
Switches .....	546
Gateways .....	550
PBXs .....	552
Firewalls .....	553
Honeypot .....	572
Network Segregation and Isolation .....	572
Networking Services and Protocols .....	573
Domain Name Service .....	573
Directory Services .....	578
Lightweight Directory Access Protocol .....	580
Network Address Translation .....	580
Intranets and Extranets .....	582
Metropolitan Area Networks .....	585
Wide Area Networks .....	586
Telecommunications Evolution .....	587
Dedicated Links .....	589
WAN Technologies .....	592
Remote Access .....	610
Dial-Up and RAS .....	610
ISDN .....	611
DSL .....	613
Cable Modems .....	613
VPN .....	615
Authentication Protocols .....	621
Remote Access Guidelines .....	623
Wireless Technologies .....	624
Wireless Communications .....	625
WLAN Components .....	627
Wireless Standards .....	630
WAP .....	641
i-Mode .....	642
Mobile Phone Security .....	643
War Driving for WLANs .....	644
Satellites .....	646
Rootkits .....	649
Spyware and Adware .....	650
Instant Messaging .....	651
Summary .....	652
Quick Tips .....	652
Questions .....	656
Answers .....	660
<b>Chapter 8</b> Cryptography .....	<b>665</b>
The History of Cryptography .....	666
Cryptography Definitions and Concepts .....	671
Kerckhoffs' Principle .....	672
The Strength of the Cryptosystem .....	674
Services of Cryptosystems .....	675
One-Time Pad .....	677
Running and Concealment Ciphers .....	679
Steganography .....	680

Types of Ciphers .....	683
Substitution Ciphers .....	683
Transposition Ciphers .....	684
Methods of Encryption .....	686
Symmetric vs. Asymmetric Algorithms .....	686
Symmetric Cryptography .....	686
Block and Stream Ciphers .....	691
Hybrid Encryption Methods .....	696
Types of Symmetric Systems .....	702
Data Encryption Standard .....	703
Triple-DES .....	710
The Advanced Encryption Standard .....	711
International Data Encryption Algorithm .....	711
Blowfish .....	712
RC4 .....	712
RC5 .....	712
RC6 .....	712
Types of Asymmetric Systems .....	713
The Diffie-Hellman Algorithm .....	713
RSA .....	716
El Gamal .....	719
Elliptic Curve Cryptosystems .....	719
LUC .....	720
Knapsack .....	720
Zero Knowledge Proof .....	720
Message Integrity .....	721
The One-Way Hash .....	721
Various Hashing Algorithms .....	726
MD2 .....	727
MD4 .....	727
MD5 .....	727
Attacks Against One-Way Hash Functions .....	729
Digital Signatures .....	730
Digital Signature Standard .....	733
Public Key Infrastructure .....	733
Certificate Authorities .....	734
Certificates .....	737
The Registration Authority .....	737
PKI Steps .....	738
Key Management .....	740
Key Management Principles .....	741
Rules for Keys and Key Management .....	742
Link Encryption vs. End-to-End Encryption .....	742
E-mail Standards .....	745
Multipurpose Internet Mail Extension .....	745
Privacy-Enhanced Mail .....	746
Message Security Protocol .....	747
Pretty Good Privacy .....	747
Quantum Cryptography .....	748
Internet Security .....	750
Start with the Basics .....	750
Attacks .....	761
Cipher-Only Attacks .....	761
Known-Plaintext Attacks .....	761
Chosen-Plaintext Attacks .....	761
Chosen-Ciphertext Attacks .....	762

	Differential Cryptanalysis .....	762
	Linear Cryptanalysis .....	763
	Side-Channel Attacks .....	763
	Replay Attacks .....	764
	Algebraic Attacks .....	764
	Analytic Attacks .....	764
	Statistical Attacks .....	764
	Summary .....	765
	Quick Tips .....	765
	Questions .....	769
	Answers .....	773
<b>Chapter 9</b>	<b>Business Continuity and Disaster Recovery .....</b>	<b>777</b>
	Business Continuity and Disaster Recovery .....	778
	Business Continuity Steps .....	780
	Making BCP Part of the Security Policy and Program .....	781
	Project Initiation .....	783
	Business Continuity Planning Requirements .....	785
	Business Impact Analysis .....	786
	Preventive Measures .....	793
	Recovery Strategies .....	794
	Business Process Recovery .....	796
	Facility Recovery .....	797
	Supply and Technology Recovery .....	803
	The End-User Environment .....	808
	Data Backup Alternatives .....	809
	Electronic Backup Solutions .....	812
	Choosing a Software Backup Facility .....	814
	Insurance .....	816
	Recovery and Restoration .....	817
	Developing Goals for the Plans .....	821
	Implementing Strategies .....	823
	Testing and Revising the Plan .....	824
	Maintaining the Plan .....	829
	Summary .....	832
	Quick Tips .....	832
	Questions .....	834
	Answers .....	840
<b>Chapter 10</b>	<b>Legal, Regulations, Compliance, and Investigations .....</b>	<b>845</b>
	The Many Facets of Cyberlaw .....	846
	The Crux of Computer Crime Laws .....	847
	Complexities in Cybercrime .....	849
	Electronic Assets .....	851
	The Evolution of Attacks .....	851
	Different Countries .....	854
	Types of Laws .....	856
	Intellectual Property Laws .....	860
	Trade Secret .....	861
	Copyright .....	861
	Trademark .....	862
	Patent .....	862
	Internal Protection of Intellectual Property .....	863
	Software Piracy .....	863
	Privacy .....	865
	Laws, Directives, and Regulations .....	866

Liability and Its Ramifications	874
Personal Information	877
Hacker Intrusion	878
Investigations	879
Incident Response	879
Incident Response Procedures	883
Computer Forensics and Proper Collection of Evidence	887
International Organization on Computer Evidence	888
Motive, Opportunity, and Means	889
Computer Criminal Behavior	890
Incident Investigators	890
The Forensics Investigation Process	892
What Is Admissible in Court?	898
Surveillance, Search, and Seizure	901
Interviewing and Interrogating	902
A Few Different Attack Types	903
Ethics	906
The Computer Ethics Institute	907
The Internet Architecture Board	908
Corporate Ethics Programs	909
Summary	910
Quick Tips	910
Questions	913
Answers	918
<b>Chapter II</b>	
Application Security	921
Software's Importance	921
Where Do We Place the Security?	922
Different Environments Demand Different Security	924
Environment vs. Application	924
Complexity of Functionality	925
Data Types, Format, and Length	926
Implementation and Default Issues	926
Failure States	928
Database Management	928
Database Management Software	929
Database Models	930
Database Programming Interfaces	935
Relational Database Components	936
Integrity	940
Database Security Issues	942
Data Warehousing and Data Mining	948
System Development	951
Management of Development	951
Life-Cycle Phases	952
Software Development Methods	968
Computer-Aided Software Engineering	969
Prototyping	970
Secure Design Methodology	970
Secure Development Methodology	971
Security Testing	972
Change Control	972
The Capability Maturity Model	974
Software Escrow	976
Application Development Methodology	976
Object-Oriented Concepts	978

	Polymorphism .....	984
	Data Modeling .....	986
	Software Architecture .....	986
	Data Structures .....	987
	Cohesion and Coupling .....	987
Distributed Computing .....		989
	CORBA and ORBs .....	989
	COM and DCOM .....	991
	Enterprise JavaBeans .....	993
	Object Linking and Embedding .....	993
	Distributed Computing Environment .....	994
Expert Systems and Knowledge-Based Systems .....		995
Artificial Neural Networks .....		998
Web Security .....		1000
	Vandalism .....	1000
	Financial Fraud .....	1001
	Privileged Access .....	1001
	Theft of Transaction Information .....	1001
	Theft of Intellectual Property .....	1001
	Denial-of-Service (DoS) Attacks .....	1001
	Create a Quality Assurance Process .....	1002
	Web Application Firewalls .....	1002
	Intrusion Prevention Systems .....	1002
	Implement SYN Proxies on the Firewall .....	1003
	Specific Threats for Web Environments .....	1003
Mobile Code .....		1013
	Java Applets .....	1013
	ActiveX Controls .....	1015
	Malicious Software (Malware) .....	1016
	Antivirus Software .....	1022
	Spam Detection .....	1025
	Anti-Malware Programs .....	1026
Patch Management .....		1027
	Step 1: Infrastructure .....	1028
	Step 2: Research .....	1028
	Step 3: Assess and Test .....	1028
	Step 4: Mitigation (“Rollback”) .....	1029
	Step 5: Deployment (“Rollout”) .....	1029
	Step 6: Validation, Reporting, and Logging .....	1029
	Limitations to Patching .....	1030
	Best Practices .....	1030
	Anything Else? .....	1030
	Attacks .....	1031
Summary .....		1035
Quick Tips .....		1036
	Questions .....	1040
	Answers .....	1044
<b>Chapter 12</b>	<b>Operations Security .....</b>	<b>1049</b>
	The Role of the Operations Department .....	1050
	Administrative Management .....	1051
	Security and Network Personnel .....	1053
	Accountability .....	1055
	Clipping Levels .....	1055
	Assurance Levels .....	1056
	Operational Responsibilities .....	1056
	Unusual or Unexplained Occurrences .....	1057

	Deviations from Standards .....	1057
	Unscheduled Initial Program Loads (a.k.a. Rebooting) .....	1058
	Asset Identification and Management .....	1058
	System Controls .....	1059
	Trusted Recovery .....	1060
	Input and Output Controls .....	1062
	System Hardening .....	1063
	Remote Access Security .....	1066
	Configuration Management .....	1067
	Change Control Process .....	1067
	Change Control Documentation .....	1069
	Media Controls .....	1070
	Data Leakage .....	1077
	Network and Resource Availability .....	1079
	Mean Time Between Failures (MTBF) .....	1080
	Mean Time to Repair (MTTR) .....	1080
	Single Points of Failure .....	1081
	Backups .....	1089
	Contingency Planning .....	1092
	Mainframes .....	1093
	E-mail Security .....	1095
	How E-mail Works .....	1096
	Facsimile Security .....	1099
	Hack and Attack Methods .....	1101
	Vulnerability Testing .....	1110
	Penetration Testing .....	1113
	Wardialing .....	1117
	Other Vulnerability Types .....	1118
	Postmortem .....	1120
	Summary .....	1122
	Quick Tips .....	1122
	Questions .....	1124
	Answers .....	1130
<b>Appendix A</b>	Security Content Automation Protocol Overview .....	<b>1133</b>
	Background .....	1133
	SCAP—More Than Just a Protocol .....	1134
	A Vulnerability Management Problem .....	1134
	A Vulnerability Management Solution—SCAP and SCAP Specifications .....	1136
	SCAP Product Validation Program .....	1138
	The Future of Security Automation .....	1139
	Conclusion .....	1139
<b>Appendix B</b>	About the CD-ROM .....	<b>1141</b>
	Running the QuickTime Cryptography Video Sample .....	1142
	Troubleshooting .....	1143
	Installing Total Seminars' Test Software .....	1143
	Navigation .....	1143
	Practice Mode .....	1143
	Final Mode .....	1143
	Minimum System Requirements for Total Seminars' Software .....	1144
	Technical Support .....	1144
	Glossary .....	<b>1145</b>
	Index .....	<b>1161</b>