

# Contents at a Glance

---

<b><i>Introduction</i></b> .....	<b>1</b>
<b><i>Part I: Certification Basics</i></b> .....	<b>7</b>
Chapter 1: (ISC) <sup>2</sup> and the CISSP Certification.....	9
Chapter 2: The Common Body of Knowledge (CBK).....	19
Chapter 3: Putting Your Certification to Good Use .....	27
<b><i>Part II: Domains</i></b> .....	<b>43</b>
Chapter 4: Access Control.....	45
Chapter 5: Application Development Security.....	89
Chapter 6: Business Continuity and Disaster Recovery Planning.....	135
Chapter 7: Cryptography .....	175
Chapter 8: Information Security Governance and Risk Management.....	213
Chapter 9: Legal, Regulations, Investigations, and Compliance.....	245
Chapter 10: Operations Security .....	283
Chapter 11: Physical (Environmental) Security.....	313
Chapter 12: Security Architecture and Design.....	337
Chapter 13: Telecommunications and Network Security.....	363
<b><i>Part III: The Part of Tens</i></b> .....	<b>427</b>
Chapter 14: Ten Test Preparation Tips.....	429
Chapter 15: Ten Test Day Tips.....	435
Chapter 16: Ten Points to Remember from Each of the Ten Domains .....	439
Chapter 17: Ten More Sources for Security Certifications.....	457
Chapter 18: Ten Security Web Sites .....	469
Chapter 19: Ten Essential Reference Books .....	473
<b><i>Part IV: Appendixes</i></b> .....	<b>475</b>
Appendix A: About the CD-ROM .....	477
Appendix B: Sample CISSP Study Questions .....	479
Appendix C: Practice Answer Sheets .....	515
Appendix D: Glossary.....	523
<b><i>Index</i></b> .....	<b>555</b>



# Table of Contents

.....

<b><i>Introduction</i></b> .....	<b>1</b>
About This Book .....	2
A Note about This Edition .....	2
How This Book Is Organized .....	3
Part I: Certification Basics .....	3
Part II: Domains .....	3
Part III: The Part of Tens .....	3
Part IV: Appendixes .....	4
How the Chapters Are Organized .....	4
Chapter introductions .....	4
Study subjects .....	5
Tables and illustrations .....	5
Prep Tests .....	5
Icons Used in This Book .....	5
Let's Get Started! .....	6

## ***Part I: Certification Basics***..... **7**

### **Chapter 1: (ISC)<sup>2</sup> and the CISSP Certification** . . . . . **9**

About (ISC) <sup>2</sup> and the CISSP Certification .....	9
You Must Be This Tall to Ride (And Other Requirements).....	10
Registering for the Exam .....	11
Preparing for the Exam .....	12
Studying on your own .....	13
Getting hands-on experience.....	13
Attending an (ISC) <sup>2</sup> CISSP CBK Review Seminar.....	14
Attending other training courses or study groups.....	14
Are you ready for the exam? .....	15
About the CISSP Examination .....	15
Waiting for Your Results.....	17

### **Chapter 2: The Common Body of Knowledge (CBK)**. . . . . **19**

Access Control .....	19
Application Development Security.....	20
Business Continuity and Disaster Recovery Planning .....	21
Cryptography .....	21
Information Security Governance and Risk Management .....	22
Legal, Regulations, Investigations, and Compliance .....	23
Operations Security .....	23
Physical (Environmental) Security.....	24
Security Architecture and Design.....	24
Telecommunications and Network Security .....	25

<b>Chapter 3: Putting Your Certification to Good Use . . . . .</b>	<b>27</b>
Following the (ISC) <sup>2</sup> Code of Ethics . . . . .	28
Keeping Your Certification Current . . . . .	29
Remaining an Active (ISC) <sup>2</sup> Member . . . . .	30
Considering (ISC) <sup>2</sup> Volunteer Opportunities . . . . .	31
Writing certification exam questions . . . . .	31
Speaking at events . . . . .	31
Supervising examinations . . . . .	32
Writing articles for the (ISC) <sup>2</sup> Journal or (ISC) <sup>2</sup> Newsletter . . . . .	32
Contribute to the (ISC) <sup>2</sup> Cyber Exchange . . . . .	32
Participating in (ISC) <sup>2</sup> focus groups . . . . .	33
Getting involved with a study group . . . . .	33
Becoming an Active Member of Your Local Security Chapter . . . . .	33
Spreading the Good Word about CISSP Certification . . . . .	34
Promoting other certifications . . . . .	35
Wearing the colors proudly . . . . .	35
Using Your CISSP Certification to Be an Agent of Change . . . . .	36
Earning Other Certifications . . . . .	36
Other (ISC) <sup>2</sup> certifications . . . . .	37
CISSP concentrations . . . . .	37
Non-(ISC) <sup>2</sup> certifications . . . . .	37
Choosing the right certifications . . . . .	40
Pursue Security Excellence . . . . .	40

## ***Part II: Domains* . . . . . 43**

<b>Chapter 4: Access Control . . . . .</b>	<b>45</b>
Basic Concepts of Access Control . . . . .	46
Control Types and Purposes . . . . .	47
Administrative controls . . . . .	48
Technical controls . . . . .	49
Physical controls . . . . .	49
Access Control Services . . . . .	50
Authentication . . . . .	50
Authorization . . . . .	51
Accountability . . . . .	51
Categories of Access Control . . . . .	51
System access controls . . . . .	52
Data access controls . . . . .	78
Evaluating and Testing Access Controls . . . . .	83
Why test? . . . . .	83
When and how to test . . . . .	84

---

<b>Chapter 5: Application Development Security . . . . .</b>	<b>89</b>
Distributed Applications . . . . .	89
Security in distributed systems . . . . .	90
Working with agents in distributed systems . . . . .	91
Adding applets to the mix . . . . .	92
Object-Oriented Environments . . . . .	94
Databases . . . . .	96
Database security . . . . .	97
Data dictionaries . . . . .	98
Data warehouses . . . . .	98
Types of databases . . . . .	99
Database transactions . . . . .	101
Knowledge-Based Systems . . . . .	102
Expert systems . . . . .	102
Neural networks . . . . .	103
Systems Development Life Cycle . . . . .	103
Conceptual definition . . . . .	105
Functional requirements . . . . .	105
Functional specifications . . . . .	106
Design . . . . .	106
Design review . . . . .	106
Coding . . . . .	107
Code review . . . . .	107
Unit test . . . . .	108
System test . . . . .	108
Certification & accreditation . . . . .	109
Maintenance . . . . .	109
Notes about the life cycle . . . . .	110
Other systems development life cycle models . . . . .	111
Security principles in software development . . . . .	111
Application Security Controls . . . . .	112
Process isolation . . . . .	112
Hardware segmentation . . . . .	112
Separation of privilege . . . . .	113
Accountability . . . . .	113
Defense in depth . . . . .	113
Abstraction . . . . .	114
Data hiding . . . . .	114
System high mode . . . . .	114
Security kernel . . . . .	114
Reference monitor . . . . .	114
Supervisor and User modes . . . . .	115
Service Level Agreements (SLAs) . . . . .	115

System Attack Methods .....	117
Malicious code .....	117
Denial of Service.....	121
Dictionary attacks.....	122
Spoofing.....	123
Spam.....	123
Social engineering.....	124
Pseudo flaw.....	126
Remote maintenance.....	126
Maintenance hooks.....	127
Sniffing and eavesdropping .....	127
Traffic analysis and inference .....	127
Brute force.....	128
Antivirus Software.....	128
Heuristics.....	129
AV popping up everywhere.....	129
Perpetrators .....	130
Hackers.....	130
Script kiddies.....	130
Virus writers.....	131
Bot herders.....	131
Phreakers.....	131
Black hats and white hats.....	131

## **Chapter 6: Business Continuity and Disaster Recovery Planning..... 135**

Defining Disastrous Events.....	136
Natural disasters.....	136
Man-made disasters.....	137
How disasters affect businesses.....	138
How BCP and DRP Work Together .....	139
COOPeration is the key.....	141
Understanding BCP Project Elements.....	141
Determining BCP Scope .....	142
Conducting the Business Impact Assessment .....	143
Vulnerability Assessment .....	143
Criticality Assessment.....	144
Identifying key players .....	145
Establishing Maximum Tolerable Downtime.....	146
Establish recovery targets.....	147
Defining Resource Requirements.....	150
Identifying the Elements of a Business Continuity Plan .....	150
Emergency response .....	151
Damage assessment .....	151
Personnel safety.....	151
Personnel notification .....	151
Backups and off-site storage .....	152
Software escrow agreements .....	153
External communications .....	154

- Utilities ..... 154
- Logistics and supplies ..... 155
- Fire and water protection ..... 155
- Documentation ..... 156
- Data processing continuity planning ..... 156
- Developing the BCP Plan ..... 158
  - Making your BCP project a success ..... 158
  - Simplifying large or complex critical functions ..... 159
  - Documenting the strategy ..... 160
- Implementing the Business Continuity Plan ..... 161
  - Securing senior management approval ..... 161
  - Promoting organizational awareness ..... 162
  - Maintaining the plan ..... 162
- Disaster Recovery Planning ..... 162
- Developing a Disaster Recovery Plan ..... 163
  - Preparing for emergency response ..... 163
  - Notifying personnel ..... 165
  - Facilitating external communications ..... 166
  - Maintaining physical and logical security ..... 166
  - Personnel safety ..... 167
- Testing the Disaster Recovery Plan ..... 167
  - Checklist ..... 168
  - Structured walkthrough ..... 168
  - Simulation ..... 168
  - Parallel ..... 169
  - Interruption (or cutover) ..... 170

**Chapter 7: Cryptography ..... 175**

- The Role of Cryptography in Information Security ..... 176
- Cryptography Basics ..... 177
  - Plaintext and ciphertext ..... 178
  - Encryption and decryption ..... 178
  - Putting it all together: The cryptosystem ..... 180
  - Classes of ciphers ..... 181
  - Types of ciphers ..... 182
- Cryptography Alternatives ..... 184
  - Steganography: A picture is worth a thousand (hidden) words ..... 184
  - Digital watermarking: The (ouch) low watermark ..... 185
- Not Quite the Metric System: Symmetric and Asymmetric Key Systems ..... 185
  - Symmetric key cryptography ..... 185
  - Asymmetric key cryptography ..... 192
- Message Authentication ..... 195
  - Digital signatures ..... 196
  - Message digests ..... 196
- Public Key Infrastructure (PKI) ..... 199
- Key Management Functions ..... 199
- Key Escrow and Key Recovery ..... 200

E-Mail Security Applications .....	201
Internet Security Applications .....	202
Secure Sockets Layer (SSL)/Transport Layer Security (TLS) .....	202
Secure Hypertext Transfer Protocol (S-HTTP) .....	203
IPSec .....	203
Multi-Protocol Label Switching (MPLS) .....	205
Secure Shell (SSH-2).....	205
Wireless Transport Layer Security (WTLS).....	205
Methods of Attack .....	206
The Birthday Attack .....	207
Ciphertext Only Attack (COA).....	207
Chosen Text Attack (CTA).....	207
Known Plaintext Attack (KPA) .....	208
Man-in-the-Middle Attack.....	208
Meet-in-the-Middle Attack.....	208
Replay Attack .....	208

## **Chapter 8: Information Security Governance and Risk Management . . . . . 213**

Information Security Governance Concepts and Principles .....	213
Confidentiality .....	214
Integrity .....	215
Availability .....	215
Defense-in-depth .....	216
Avoiding single points of failure .....	216
Data Classification .....	218
Commercial data classification .....	218
Government data classification .....	219
Mission Statements, Goals, and Objectives .....	220
Mission (not so impossible) .....	220
Goals and objectives .....	220
Policies, Standards, Guidelines, and Procedures .....	221
Policies .....	221
Standards (and baselines) .....	222
Guidelines .....	222
Procedures.....	222
Information Security Governance Practices .....	223
Outsourcing.....	223
Internal Service Level Agreements (SLAs) .....	223
Identity management.....	223
Certification and accreditation .....	224
Personnel Security Policies and Practices .....	224
Background checks and security clearances .....	224
Employment agreements .....	225
Hiring and termination practices.....	225
Job descriptions.....	226
Security roles and responsibilities .....	226
Separation of duties and responsibilities .....	228
Job rotation .....	229

Risk Management Concepts ..... 229  
 Risk identification ..... 230  
 Risk Analysis (RA)..... 232  
 Risk treatment ..... 234  
 Security Education, Training, and Awareness Programs ..... 236  
 Awareness..... 237  
 Training ..... 238  
 Education ..... 238  
 Professional Ethics ..... 238  
 (ISC)<sup>2</sup> Code of Ethics..... 239  
 Internet Architecture Board (IAB) —  
 Ethics and the Internet (RFC 1087) ..... 240  
 Computer Ethics Institute (CEI)..... 241

**Chapter 9: Legal, Regulations, Investigations,  
 and Compliance ..... 245**

Major Types and Classifications of Law ..... 245  
 Common law ..... 245  
 International law ..... 249  
 Major Categories of Computer Crime ..... 250  
 Terrorist attacks ..... 252  
 Military and intelligence attacks..... 252  
 Financial attacks ..... 252  
 Business attacks..... 252  
 Grudge attacks ..... 253  
 “Fun” attacks ..... 253  
 Types of Laws Relevant to Computer Crimes..... 254  
 Intellectual property..... 254  
 Privacy and data protection laws ..... 256  
 Disclosure laws ..... 261  
 Computer crime and information security laws ..... 263  
 Investigations ..... 269  
 Evidence..... 270  
 Conducting investigations ..... 277  
 Incident handling (or response) ..... 278

**Chapter 10: Operations Security ..... 283**

Administrative Management and Control ..... 283  
 Job requirements and qualifications ..... 284  
 Background checks and verification ..... 284  
 Separation of duties and responsibilities ..... 286  
 Job rotation ..... 287  
 Mandatory vacations..... 287  
 Need-to-know..... 288  
 Least privilege ..... 288  
 User monitoring ..... 289  
 Termination of employment..... 290

Security Operations Concepts .....	290
Handling sensitive information .....	290
Records retention .....	291
Threats and Countermeasures .....	292
Errors and Omissions .....	292
Fraud .....	292
Hackers and crackers .....	293
Industrial espionage .....	293
Loss of physical and infrastructure support .....	294
Malicious code .....	294
Sabotage .....	294
Theft .....	294
Security Controls .....	294
Resource protection .....	295
Privileged entity controls .....	296
Change controls .....	296
Media controls .....	297
Administrative controls .....	297
Trusted recovery .....	298
Security Auditing and Due Care .....	298
Audit Trails .....	298
Anatomy of an audit record .....	299
Types of audit trails .....	299
How to go looking for trouble .....	300
Problem management and audit trails .....	300
Retaining audit logs .....	301
Protection of audit logs .....	301
Monitoring .....	302
Penetration testing .....	302
Intrusion detection and prevention .....	304
Violation analysis .....	305
Keystroke monitoring .....	305
Traffic and trend analysis .....	305
Facilities monitoring .....	306
Responding to events .....	306
<b>Chapter 11: Physical (Environmental) Security .....</b>	<b>313</b>
Physical Security Threats .....	313
Site and Facility Design Considerations .....	317
Choosing a secure location .....	318
Designing a secure facility .....	319
Physical (Environmental) Security Controls .....	320
Physical access controls .....	320
Technical controls .....	324
Environmental and life safety controls .....	326
Administrative controls .....	331
Bringing It All Together .....	332

<b>Chapter 12: Security Architecture and Design . . . . .</b>	<b>337</b>
Computer Architecture.....	337
Hardware.....	338
Firmware .....	343
Software .....	343
Security Architecture.....	345
Trusted Computing Base (TCB).....	345
Open and closed systems .....	346
Protection rings .....	347
Security modes.....	347
Recovery procedures .....	348
Issues in security architectures .....	348
Access Control Models .....	350
Bell-La Padula .....	350
Access Matrix .....	351
Take-Grant .....	351
Biba.....	351
Clark-Wilson.....	352
Information Flow.....	352
Non-interference .....	352
Evaluation Criteria.....	352
Trusted Computer System Evaluation Criteria (TCSEC) .....	353
Trusted Network Interpretation (TNI) .....	356
European Information Technology Security Evaluation Criteria (ITSEC) .....	356
Common Criteria.....	357
System Certification and Accreditation.....	358
DITSCAP .....	359
NIACAP .....	359
DCID 6/3.....	359
<b>Chapter 13: Telecommunications and Network Security. . . . .</b>	<b>363</b>
Data Network Types .....	363
Local area network (LAN).....	363
Wide area network (WAN).....	364
The OSI Reference Model .....	366
Physical Layer (Layer 1) .....	368
Data Link Layer (Layer 2) .....	377
Network Layer (Layer 3).....	388
Transport Layer (Layer 4).....	393
Session Layer (Layer 5).....	396
Presentation Layer (Layer 6).....	397
Application Layer (Layer 7).....	398
The TCP/IP Model.....	400

Network Security .....	401
Firewalls .....	401
Intrusion detection and prevention systems (IDSs, IPSs, and IDPSs).....	406
Remote access.....	407
Virtual Private Networks (VPNs) .....	409
Wireless Network (WLAN) Security .....	412
WLAN components and architectures .....	412
WLAN security techniques and protocols.....	413
E-mail, Web, Facsimile, and Telephone Security .....	415
E-mail security.....	415
Web security.....	418
Facsimile security .....	418
PBX fraud and abuse .....	419
Caller ID fraud and abuse.....	419
Network Attacks and Countermeasures .....	420
Bluejacking and bluesnarfing .....	420
Fraggle.....	420
ICMP flood.....	421
Session hijacking (spoofing).....	421
Smurf .....	421
SYN flood.....	421
Teardrop .....	422
UDP flood .....	422

## ***Part III: The Part of Tens* ..... 427**

### **Chapter 14: Ten Test Preparation Tips ..... 429**

Get a Networking Certification First.....	429
Register NOW!.....	430
Make a 60-Day Study Plan.....	430
Get Organized and READ! .....	430
Join a Study Group .....	431
Take Practice Exams .....	431
Take a CISSP Review Seminar .....	432
Develop a Test-Taking Strategy .....	432
Practice Drawing Circles .....	433
Plan Your Travel.....	433

### **Chapter 15: Ten Test Day Tips ..... 435**

Get a Good Night's Rest.....	435
Dress Comfortably (And Appropriately).....	435
Eat a Good Breakfast.....	436

Arrive Early .....	436
Bring Your Registration Letter and ID .....	436
Bring Snacks and Drinks .....	436
Bring Prescription or Over-the-Counter Medications.....	437
Bring Extra Pencils and a BIG Eraser .....	437
Leave Your Cell Phone, Pager, PDA, and Digital Watch Behind .....	437
Take Frequent Breaks .....	438

### **Chapter 16: Ten Points to Remember from Each of the Ten Domains . . . . . 439**

Access Control.....	439
Application Development Security.....	440
Business Continuity and Disaster Recovery Planning .....	442
Cryptography .....	443
Information Security Governance and Risk Management .....	444
Legal, Regulations, Investigations, and Compliance.....	446
Operations Security .....	449
Physical (Environmental) Security.....	450
Security Architecture and Design.....	453
Telecommunications and Network Security.....	454

### **Chapter 17: Ten More Sources for Security Certifications. . . . . 457**

ASIS International .....	457
Check Point .....	458
Cisco.....	458
CompTIA .....	459
DRI International.....	460
EC-Council .....	461
ISACA.....	462
CISA.....	462
CISM.....	462
CGEIT.....	463
(ISC) <sup>2</sup> .....	463
SSCP .....	463
CSSLP .....	464
CAP .....	465
CISSP concentrations .....	465
Microsoft.....	466
SANS/GIAC .....	467

### **Chapter 18: Ten Security Web Sites . . . . . 469**

CISSP Open Study Guide.....	469
Carnegie Mellon SEI CERT Coordination Center .....	469
Common Vulnerabilities and Exposures .....	470
Hieros Gamos (HG) Guide to Computers and the Law .....	470

INFOSYSSEC.....	470
National Institute of Standards and Technology.....	470
Simovits Consulting.....	471
Slashdot .....	471
The SANS Institute.....	471
WindowSecurity Network Security Library.....	472
<b>Chapter 19: Ten Essential Reference Books .....</b>	<b>473</b>
<b><i>Part IV: Appendixes.....</i></b>	<b><i>475</i></b>
<b>Appendix A: About the CD-ROM .....</b>	<b>477</b>
<b>Appendix B: Sample CISSP Study Questions .....</b>	<b>479</b>
<b>Appendix C: Practice Answer Sheets .....</b>	<b>515</b>
<b>Appendix D: Glossary .....</b>	<b>523</b>
<b><i>Index.....</i></b>	<b><i>555</i></b>