

# 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 .....	25
<b><i>Part II: Domains</i></b> .....	<b>37</b>
Chapter 4: Access Control .....	39
Chapter 5: Telecommunications and Network Security .....	73
Chapter 6: Information Security and Risk Management .....	123
Chapter 7: Application Security .....	153
Chapter 8: Cryptography .....	189
Chapter 9: Security Architecture and Design .....	223
Chapter 10: Operations Security .....	247
Chapter 11: Business Continuity and Disaster Recovery Planning .....	277
Chapter 12: Legal, Regulations, Compliance, and Investigations .....	303
Chapter 13: Physical (Environmental) Security .....	339
<b><i>Part III: The Part of Tens</i></b> .....	<b>363</b>
Chapter 14: Ten Test Preparation Tips .....	365
Chapter 15: Ten Test Day Tips .....	371
Chapter 16: Ten More Sources for Security Certifications .....	375
<b><i>Part IV: Appendix and Bonus Chapters</i></b> .....	<b>383</b>
Appendix A: About the CD-ROM .....	385
<b><i>Index</i></b> .....	<b>387</b>



# Table of Contents

---

## ***Introduction*** ..... 1

About This Book.....	1
How This Book Is Organized.....	2
Part I: Certification Basics.....	2
Part II: Domains .....	2
Part III: The Part of Tens.....	2
Part IV: Appendixes and Bonus Chapters .....	2
How the Chapters Are Organized.....	3
Chapter introductions .....	3
Study subjects .....	3
Tables and illustrations .....	3
Prep Tests.....	4
Icons Used in This Book.....	4
Let's Get Started!.....	5

## ***Part 1: 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 Minimum Requirements) .....	10
Registering for the Exam.....	11
Developing a Study Plan.....	12
Self-study .....	13
Getting hands-on experience.....	14
Attending an (ISC) <sup>2</sup> CISSP review seminar .....	14
Attending other training courses or study groups .....	15
Are you ready for the exam?.....	15
About the CISSP Examination.....	16
Waiting for Your Results.....	17

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

Access Control.....	19
Telecommunications and Network Security.....	20
Information Security and Risk Management.....	21
Application Security .....	21
Cryptography .....	22
Security Architecture and Design .....	22
Operations Security.....	23

Business Continuity and Disaster Recovery Planning .....	23
Legal, Regulations, Compliance, and Investigations .....	24
Physical (Environmental) Security .....	24

**Chapter 3: Putting Your Certification to Good Use ..... 25**

Following the (ISC) <sup>2</sup> Code of Ethics .....	26
Keeping Your Certification Current .....	27
Remaining an Active (ISC) <sup>2</sup> Member .....	27
Considering (ISC) <sup>2</sup> Volunteer Opportunities .....	28
Writing certification exam questions .....	28
Speaking at events .....	29
Supervising examinations .....	29
Writing articles for the (ISC) <sup>2</sup> Journal or (ISC) <sup>2</sup> Newsletter .....	29
Participating in (ISC) <sup>2</sup> focus groups .....	30
Getting involved with a study group .....	30
Becoming an Active Member of Your Local Security Chapter .....	30
Spreading the Good Word about CISSP Certification .....	31
Promoting other certifications .....	32
Wearing the colors proudly .....	32
Using Your CISSP Certification to Be an Agent of Change .....	33
Earning Other Certifications .....	33
Other (ISC) <sup>2</sup> certifications .....	34
Non-(ISC) <sup>2</sup> certifications .....	34
Choosing the right certifications .....	36

**Part II: Domains ..... 37**

**Chapter 4: Access Control ..... 39**

Uncovering Concepts of Access Control .....	40
Control types .....	40
Access control services .....	42
Categories of Access Control .....	43
System access controls .....	43
Data access controls .....	63
Evaluating and Testing Access Controls .....	67
Why test? .....	67
When and how to test .....	68
Additional References .....	69

**Chapter 5: Telecommunications and Network Security ..... 73**

Data Network Types .....	73
Local area network (LAN) .....	74
Wide area network (WAN) .....	74

The OSI Reference Model .....75  
 Physical Layer (Layer 1).....76  
 Data Link Layer (Layer 2).....81  
 Network Layer (Layer 3).....92  
 Transport Layer (Layer 4).....94  
 Session Layer (Layer 5) .....97  
 Presentation Layer (Layer 6) .....98  
 Application Layer (Layer 7) .....98  
 The TCP/IP Model .....100  
 Network Security.....100  
 Firewalls.....101  
 Virtual Private Networks (VPNs).....105  
 Intrusion detection and prevention systems (IDS and IPS) .....108  
 Remote access .....109  
 E-mail, Web, Facsimile, and Telephone Security .....112  
 E-mail security .....112  
 Web security .....115  
 Facsimile security.....115  
 PBX fraud and abuse.....116  
 Caller ID fraud and abuse .....116  
 Network Attacks and Countermeasures .....117  
 SYN flood .....117  
 ICMP flood.....117  
 UDP flood.....118  
 Smurf.....118  
 Fraggle.....118  
 Teardrop .....118  
 Session hijacking (Spoofing) .....118  
 Additional References .....119

**Chapter 6: Information Security and Risk Management . . . . .123**

Information Security Management Concepts and Principles .....123  
 Confidentiality .....124  
 Integrity .....125  
 Availability.....125  
 Defense-in-depth.....125  
 Avoiding single points of failure .....126  
 Data Classification .....127  
 Commercial data classification.....127  
 Government data classification.....128  
 Mission Statements, Goals, and Objectives .....129  
 Mission (not so impossible) .....129  
 Goals and objectives .....129  
 Policies, Standards, Guidelines, and Procedures.....130  
 Policies.....131  
 Standards (and baselines).....131

Guidelines .....	131
Procedures .....	132
Information Security Management Practices .....	132
Outsourcing.....	132
Internal Service Level Agreements (SLAs).....	132
Identity management .....	132
Certification and accreditation.....	133
Personnel Security Policies and Practices.....	133
Background checks and security clearances .....	133
Employment agreements.....	134
Hiring and termination practices .....	134
Job descriptions .....	135
Security roles and responsibilities.....	135
Separation of duties and responsibilities.....	138
Job rotations .....	138
Risk Management Concepts.....	138
Risk identification.....	139
Risk analysis.....	141
Risk control .....	144
Security Education, Training, and Awareness Programs .....	146
Awareness .....	146
Training.....	147
Education .....	147
Additional References .....	148

## **Chapter 7: Application Security .....153**

Distributed Applications .....	154
Security in distributed systems.....	154
Agents .....	155
Applets.....	155
Object-Oriented Environments .....	157
Databases .....	158
Database security.....	159
Data dictionaries .....	160
Data warehouses .....	160
Knowledge-Based Systems.....	161
Expert systems .....	161
Neural networks .....	162
Systems Development Life Cycle .....	162
Conceptual definition .....	164
Functional requirements .....	164
Functional specifications .....	164
Design .....	165
Coding.....	165
Code review.....	166
Unit test .....	166

System test .....	166
Certification .....	167
Accreditation .....	167
Maintenance .....	167
Notes about the life cycle .....	168
Change Management .....	168
Configuration Management .....	169
Application Security Controls .....	169
Process isolation .....	169
Hardware segmentation .....	169
Separation of privilege .....	170
Accountability .....	170
Defense in depth .....	170
Abstraction .....	171
Data hiding .....	171
System high mode .....	171
Security kernel .....	171
Reference monitor .....	171
Supervisor and user modes .....	172
Service Level Agreements .....	172
System Attack Methods .....	173
Malicious code .....	173
Denial of Service .....	177
Dictionary attacks .....	177
Spoofing .....	178
Social engineering .....	178
Pseudo flaw .....	178
Remote maintenance .....	179
Maintenance hooks .....	179
Sniffing and eavesdropping .....	179
Traffic analysis and inference .....	180
Brute force .....	180
Antivirus software .....	180
Perpetrators .....	182
Hackers .....	182
Script kiddies .....	182
Virus writers .....	182
Bot herders .....	183
Phreakers .....	183
Black hats and white hats .....	183
Additional References .....	184
<b>Chapter 8: Cryptography .....</b>	<b>189</b>
The Role of Cryptography in Information Security .....	190
Cryptography Basics .....	191
Classes of ciphers .....	191
Types of ciphers .....	191

Key clustering .....	193
Putting it all together: The cryptosystem .....	194
Encryption and decryption .....	195
He said, she said: The concept of non-repudiation .....	196
A disposable cipher: The one-time pad .....	196
Plaintext and ciphertext .....	196
Work factor: Force x effort = work! .....	197
Cryptography Alternatives .....	197
Steganography: A picture is worth a thousand (hidden) words .....	197
Digital watermarking: The (ouch) low watermark .....	198
Not Quite the Metric System: Symmetric and Asymmetric Key Systems .....	198
Symmetric key cryptography .....	198
Asymmetric key cryptography .....	203
Message Authentication .....	207
Digital signatures .....	208
Message digests .....	208
Public Key Infrastructure (PKI) .....	210
Key Management Functions .....	210
Key generation .....	211
Key distribution .....	211
Key installation .....	211
Key storage .....	211
Key change .....	211
Key control .....	211
Key disposal .....	212
Key Escrow and Key Recovery .....	212
E-Mail Security Applications .....	212
Secure Multipurpose Internet Mail Extensions (S/MIME) .....	212
MIME Object Security Services (MOSS) .....	213
Privacy Enhanced Mail (PEM) .....	213
Pretty Good Privacy (PGP) .....	213
Internet Security Applications .....	213
Secure Sockets Layer (SSL)/Transport Layer Security (TLS) .....	214
Secure Hypertext Transfer Protocol (S-HTTP) .....	214
IPSec .....	215
Multi-Protocol Label Switching (MPLS) .....	216
Secure Shell (SSH-2) .....	216
Wireless Transport Layer Security (WTLS) .....	216
Methods of Attack .....	217
The Birthday Attack .....	217
Ciphertext Only Attack (COA) .....	218
Chosen Text Attack (CTA) .....	218
Known Plaintext Attack (KPA) .....	218
Man-in-the-Middle .....	218

---

Meet-in-the-Middle .....	219
Replay Attack .....	219
Additional References .....	219
<b>Chapter 9: Security Architecture and Design .....</b>	<b>223</b>
Computer Architecture .....	223
Hardware .....	224
Firmware.....	228
Software.....	228
Security Architecture.....	229
Trusted Computing Base (TCB) .....	229
Open and closed systems .....	230
Protection rings .....	230
Security modes .....	230
Recovery procedures.....	231
Issues in security architectures.....	231
Access Control Models .....	232
Bell-LaPadula .....	233
Access Matrix.....	233
Take-Grant .....	234
Biba .....	234
Clark-Wilson .....	234
Information Flow .....	235
Non-interference.....	235
Evaluation Criteria .....	235
Trusted Computer System Evaluation Criteria (TCSEC).....	235
Trusted Network Interpretation (TNI).....	239
European Information Technology Security Evaluation Criteria (ITSEC).....	239
Common Criteria .....	240
System Certification and Accreditation .....	241
DITSCAP.....	242
NIACAP.....	242
Additional References .....	243
<b>Chapter 10: Operations Security .....</b>	<b>247</b>
Security Operations Concepts.....	247
Antivirus and malware management .....	248
Making backups of critical information.....	248
Need-to-know .....	249
Least privilege.....	249
Privileged functions .....	250
Privacy .....	250
Legal requirements.....	251
Illegal activities .....	251

Record retention.....	252
Handling sensitive information .....	252
Remote access .....	253
Threats and Countermeasures .....	253
Errors and Omissions .....	253
Fraud .....	253
Theft.....	254
Employee sabotage .....	254
Industrial espionage.....	254
Loss of physical and infrastructure support .....	254
Hackers and crackers .....	255
Malicious code.....	255
Inappropriate employee activities .....	255
Security Operations Management.....	256
Security Controls.....	259
Resource protection.....	260
Privileged entity controls .....	260
Change controls.....	260
Media controls .....	261
Administrative controls.....	261
Trusted recovery.....	261
Security Auditing and Due Care .....	262
Audit Trails .....	262
Anatomy of an audit record .....	263
Types of audit trails .....	263
Finding trouble in them thar logs.....	264
Problem management and audit trails .....	265
Retaining audit logs.....	265
Protection of audit logs .....	266
Monitoring.....	267
Penetration testing.....	267
Intrusion detection and prevention .....	269
Violation analysis .....	270
Keystroke monitoring .....	270
Traffic and trend analysis.....	271
Facilities monitoring .....	271
Responding to events .....	271
Additional References .....	273

## **Chapter 11: Business Continuity and Disaster Recovery Planning .....277**

Defining Disastrous Events .....	278
Natural disasters .....	278
Man-made disasters .....	279
The Differences between BCP and DRP .....	279
Understanding BCP Project Elements .....	280
Determining BCP Scope.....	281

Defining the Business Impact Assessment .....	282
Vulnerability Assessment .....	282
Criticality Assessment .....	283
Identifying key players.....	283
Establishing Maximum Tolerable Downtime .....	284
Defining Resource Requirements .....	284
BCP Recovery Plan Development .....	285
Emergency response.....	285
Damage assessment .....	285
Personnel safety .....	285
Personnel notification.....	286
Backups and off-site storage.....	286
Software escrow agreements .....	287
External communications .....	287
Utilities.....	288
Logistics and supplies .....	288
Fire and water protection.....	289
Documentation .....	289
Data processing continuity planning.....	290
Developing the BCP Plan.....	291
Identifying success factors.....	292
Simplifying large or complex critical functions .....	293
Documenting the strategy.....	293
Implementing the Business Continuity Plan.....	294
Securing senior management approval .....	294
Promoting organizational awareness.....	295
Maintaining the plan .....	295
Disaster Recovery Planning.....	295
Developing a Disaster Recovery Plan.....	296
Preparing for emergency response .....	296
Notifying personnel.....	297
Facilitating external communications .....	297
Maintaining physical security.....	298
Personnel safety .....	298
Testing the Disaster Recovery Plan.....	298
Additional References .....	299

## **Chapter 12: Legal, Regulations, Compliance, and Investigations .....303**

Major Categories and Types of Laws.....	303
U.S. common law .....	304
International law.....	307
Major Categories of Computer Crime.....	307
Terrorist attacks .....	309
Military and intelligence attacks .....	310

Financial attacks .....	310
Business attacks .....	310
Grudge attacks .....	310
“Fun” attacks .....	311
Types of Laws Relevant to Computer Crimes .....	312
Intellectual property .....	312
Privacy laws .....	314
Computer crime and information security laws .....	316
Investigations .....	323
Evidence .....	324
Conducting investigations.....	330
Incident handling (Or response) .....	331
Ethics .....	333
(ISC) <sup>2</sup> Code of Ethics .....	333
Internet Architecture Board (IAB) — “Ethics and the Internet” (RFC 1087) .....	334
Additional References .....	334

### **Chapter 13: Physical (Environmental) Security . . . . . 339**

Physical Security Threats .....	340
Site and Facility Design Considerations .....	343
Choosing a secure location .....	343
Designing a secure facility.....	344
Physical (Environmental) Security Controls .....	345
Physical access controls .....	345
Technical controls.....	349
Environmental and life safety controls.....	351
Administrative controls.....	356
Bringing It All Together .....	357
Additional References .....	358

## ***Part III: The Part of Tens* . . . . . 363**

### **Chapter 14: Ten Test Preparation Tips . . . . . 365**

Get a Networking Certification First .....	365
Register NOW!.....	365
Make a 60-Day Study Plan .....	366
Get Organized and READ!.....	366
Join a Study Group.....	367
Take Practice Exams .....	367
Take a CISSP Review Seminar .....	368
Develop a Test-Taking Strategy .....	368
Practice Drawing Circles! .....	369
Plan Your Travel.....	369

---

<b>Chapter 15: Ten Test Day Tips</b> .....	<b>371</b>
Get a Good Night's Rest.....	371
Dress Comfortably (And Appropriately).....	371
Eat a Good Breakfast.....	372
Arrive Early .....	372
Bring Your Registration Letter and ID .....	372
Bring Snacks and Drinks.....	372
Bring Prescription or Over-the-Counter Medications .....	373
Bring Extra Pencils and a BIG Eraser .....	373
Leave Your Cell Phone, Pager, PDA, and Digital Watch Behind.....	373
Take Frequent Breaks .....	374
<b>Chapter 16: Ten More Sources for Security Certifications</b> .....	<b>375</b>
ASIS International.....	375
Check Point .....	376
Cisco .....	376
CompTIA.....	377
DRI International .....	378
EC-Council.....	379
ISACA .....	379
(ISC) <sup>2</sup> .....	380
Microsoft .....	381
SANS/GIAC.....	381
<b><i>Part IV: Appendix and Bonus Chapters</i></b> .....	<b>383</b>
<b>Appendix A: About the CD-ROM</b> .....	<b>385</b>
System Requirements .....	385
Contents .....	385
If You Have Problems (Of the CD Kind).....	386
<b><i>Index</i></b> .....	<b>387</b>

