CISSP® Study Guide
## Contents

Acknowledgments .................................................................................................................. xvii
About the authors ................................................................................................................ xix

### CHAPTER 1 Introduction ........................................................................ 1
How to Prepare for the Exam ......................................................................................... 2
The Notes Card Approach .............................................................................................. 2
Practice Tests .................................................................................................................. 2
Read the Glossary ........................................................................................................... 3
Readiness Checklist ......................................................................................................... 3
How to Take the Exam ................................................................................................. 3
Steps to Becoming a CISSP® ....................................................................................... 3
Exam Logistics ............................................................................................................... 4
How to Take the Exam ................................................................................................. 5
After the Exam .............................................................................................................. 6
Good Luck! .................................................................................................................... 6

### CHAPTER 2 Domain 1: Information security governance and risk management ................................................................................................. 7
Unique Terms and Definitions ......................................................................................... 7
Introduction ..................................................................................................................... 7
Cornerstone Information Security Concepts ................................................................. 8
Confidentiality, Integrity, and Availability ..................................................................... 8
Identity and Authentication, Authorization, and Accountability ................................... 10
Risk Analysis .................................................................................................................. 13
Assets .............................................................................................................................. 13
Threats and Vulnerabilities ............................................................................................ 13
Risk = Threat × Vulnerability ....................................................................................... 14
Impact ............................................................................................................................... 15
Risk Analysis Matrix ................................................................................................... 15
Calculating Annualized Loss Expectancy .................................................................. 16
Total Cost of Ownership .............................................................................................. 17
Return on Investment ................................................................................................... 18
Risk Choices ................................................................................................................... 19
Qualitative and Quantitative Risk Analysis ................................................................. 20
The Risk Management Process .................................................................................... 21
Information Security Governance ................................................................................. 22
CHAPTER 3  Domain 2: Access control ................................. 37

Unique Terms and Definitions ........................................... 37
Introduction ........................................................................ 37
Cornerstone Access Control Concepts ............................... 38
The CIA triad ..................................................................... 38
Identification and AAA ..................................................... 40
Subjects and objects ......................................................... 41
Access Control Models ..................................................... 41
Discretionary Access Controls (DAC) ............................... 42
Mandatory Access Controls (MAC) ................................. 42
Non-Discretionary Access Control ................................. 42
Content and Context-Dependent Access Controls .......... 44
Centralized Access Control ............................................ 44
Decentralized Access Control ........................................ 44
Access Control Protocols and Frameworks ........................ 45
Procedural Issues for Access Control .............................. 47
Labels, Clearance, Formal Access Approval, and Need to
Know .............................................................................. 48
Rule-Based Access Controls ........................................ 50
Access Control Lists .......................................................... 50
Access Control Defensive Categories and Types .............. 50
Preventive ........................................................................... 51
Detective ............................................................................ 51
Corrective ............................................................................ 51
Recovery .............................................................................. 52
Modular Math ................................................................. 93
Exclusive Or (XOR) .......................................................... 93
Types of Cryptography ..................................................... 95
History of Cryptography .................................................. 95
Egyptian Hieroglyphics .................................................... 95
Spartan Scytale ............................................................... 96
Caesar Cipher and other Rotation Ciphers ......................... 96
Vigenère Cipher ............................................................... 97
Cipher Disk ....................................................................... 97
Jefferson Disks .................................................................. 98
Book Cipher and Running-Key Cipher .............................. 100
Codebooks ...................................................................... 100
One-Time Pad .................................................................. 100
Hebern Machines and Purple .......................................... 102
Cryptography Laws ......................................................... 105
Symmetric Encryption ..................................................... 105
Stream and Block Ciphers ................................................. 106
Initialization Vectors and Chaining ................................. 106
Data Encryption Standard ................................................. 106
International Data Encryption Algorithm (IDEA) ............... 110
Advanced Encryption Standard (AES) ............................ 110
Blowfish and Twofish ....................................................... 113
RC5 and RC6 ................................................................... 113
Asymmetric Encryption ................................................... 113
Asymmetric Methods ....................................................... 114
Hash Functions .................................................................. 116
Collisions ........................................................................ 116
MD5 ............................................................................... 116
Secure Hash Algorithm .................................................... 116
HAVAL ............................................................................ 117
Cryptographic Attacks .................................................... 117
Brute Force ..................................................................... 117
Known Plaintext .............................................................. 117
Chosen Plaintext and Adaptive Chosen Plaintext ............... 118
Chosen Ciphertext and Adaptive Chosen Ciphertext ......... 118
Meet-in-the-middle Attack ............................................... 118
Known Key ..................................................................... 119
Differential Cryptanalysis ............................................... 119
Linear Cryptanalysis ........................................................ 119
Side-channel Attacks ....................................................... 119
Birthday Attack ................................................................. 119
Key Clustering ..................................................................... 120
Implementing Cryptography ................................................. 120
Digital Signatures ............................................................... 120
HMAC ............................................................................. 121
CBC-MAC ........................................................................ 122
Public Key Infrastructure ................................................... 122
IPsec ................................................................................ 122
SSL and TLS .................................................................. 124
PGP .................................................................................. 124
S/MIME ............................................................................ 125
Escrowed Encryption ....................................................... 125
Steganography ................................................................ 125
Digital Watermarks .......................................................... 126
Summary of Exam Objectives ............................................. 127
Self Test ........................................................................... 127
Self Test Quick Answer Key .............................................. 129

CHAPTER 5 Domain 4: Physical (Environmental) security ........... 131
Unique Terms and Definitions .............................................. 131
Introduction ....................................................................... 131
Perimeter Defenses .......................................................... 132
Fences ............................................................................. 132
Gates .............................................................................. 132
Bollards ......................................................................... 132
Lights ............................................................................. 133
CCTV ............................................................................. 133
Locks .............................................................................. 135
Smart Cards and Magnetic Stripe Cards ......................... 138
Tailgating/piggybacking .................................................... 138
Mantraps and Turnstiles ..................................................... 140
Contraband Checks .......................................................... 140
Motion Detectors and Other Perimeter Alarms ................. 140
Doors and Windows ......................................................... 141
Walls, floors, and ceilings ................................................ 142
Guards ........................................................................... 142
Dogs ............................................................................... 143
Restricted Areas and Escorts ........................................... 143
Site Selection, Design, and Configuration ....................... 144
Site Selection Issues ......................................................... 144
Site Design and Configuration Issues ............................... 144
### Chapter 7: Domain 6: Business continuity and disaster recovery planning

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Terms and Definitions</td>
<td>211</td>
</tr>
<tr>
<td>Introduction</td>
<td>211</td>
</tr>
<tr>
<td>BCP and DRP Overview and Process</td>
<td>212</td>
</tr>
<tr>
<td>Business Continuity Planning (BCP)</td>
<td>212</td>
</tr>
<tr>
<td>Disaster Recovery Planning (DRP)</td>
<td>213</td>
</tr>
</tbody>
</table>
Network Access, Internet and Transport Layer Protocols and Concepts ........................................... 263
Application Layer TCP/IP Protocols and Concepts ................................................................. 276
Layer 1 Network Cabling ............................................................................................................. 281
LAN Technologies and Protocols ......................................................................................... 283
LAN Physical Network Topologies ....................................................................................... 285
WAN Technologies and Protocols ......................................................................................... 288
Network Devices and Protocols ............................................................................................ 291
Repeaters and Hubs ................................................................................................................. 291
Bridges .................................................................................................................................... 292
Switches .................................................................................................................................... 293
TAPs .......................................................................................................................................... 294
Routers ....................................................................................................................................... 295
Firewalls ..................................................................................................................................... 299
Modem ...................................................................................................................................... 306
DTE/DCE and CSU/DSU ............................................................................................................. 306
Intrusion Detection Systems and Intrusion
Prevention Systems ............................................................................................................... 306
Honeypots .................................................................................................................................. 309
Network Attacks ..................................................................................................................... 310
Network Scanning Tools .......................................................................................................... 311
Secure Communications ........................................................................................................... 312
Authentication Protocols and Frameworks .............................................................................. 312
VPN ......................................................................................................................................... 314
VoIP .......................................................................................................................................... 316
Wireless Local Area Networks ............................................................................................... 317
RFID .......................................................................................................................................... 321
Remote Access .......................................................................................................................... 322
Summary of Exam Objectives .................................................................................................. 324
Self Test ..................................................................................................................................... 325
Self Test Quick Answer Key .................................................................................................... 327

CHAPTER 9 Domain 8: Application development security ......................................................... 329
Unique Terms and Definitions ................................................................................................... 329
Introduction ................................................................................................................................ 329
Programming Concepts ........................................................................................................... 330
Machine Code, Source Code, and Assemblers ........................................................................ 330
Compilers, Interpreters, and Bytecode ..................................................................................... 330
Procedural and Object-Oriented Languages ......................................................................... 331
Fourth-generation Programming Language ............................................................................ 333
Computer-Aided Software Engineering (CASE) .................................................................... 333
CHAPTER 11 Domain 10: Legal regulations, investigations, and compliance

Unique Terms and Definitions.............................................. 405
Introduction............................................................................... 406
Major Legal Systems........................................................ 406
Civil Law (legal system)................................................ 406
Common Law........................................................................... 406
Religious Law......................................................................... 407
Other Systems......................................................................... 407
Criminal, Civil, and Administrative Law............................ 407
Criminal Law.......................................................................... 408
Civil Law ................................................................................ 408
Administrative Law .............................................................. 409
Information Security Aspects of Law.................................... 409
Computer Crime ...................................................................... 410
Intellectual Property .............................................................. 411
Import/export Restrictions.................................................. 415
Privacy .................................................................................... 416
Liability ................................................................................ 419
Legal Aspects of Investigations............................................ 420
Digital Forensics..................................................................... 420
Incident Response................................................................. 423
Evidence................................................................................. 423
Evidence Integrity ................................................................. 425
Chain of Custody................................................................. 426
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasonable Searches</td>
<td>426</td>
</tr>
<tr>
<td>Entrapment and enticement</td>
<td>428</td>
</tr>
<tr>
<td>Important Laws and Regulations</td>
<td>429</td>
</tr>
<tr>
<td>U.S. Computer Fraud and Abuse Act</td>
<td>430</td>
</tr>
<tr>
<td>USA PATRIOT Act</td>
<td>431</td>
</tr>
<tr>
<td>HIPAA</td>
<td>431</td>
</tr>
<tr>
<td>United States Breach Notification Laws</td>
<td>432</td>
</tr>
<tr>
<td>Ethics</td>
<td>433</td>
</tr>
<tr>
<td>Computer Ethics Institute</td>
<td>433</td>
</tr>
<tr>
<td>IAB’s Ethics and the Internet</td>
<td>434</td>
</tr>
<tr>
<td>The (ISC)² Code of Ethics</td>
<td>434</td>
</tr>
<tr>
<td>Summary of Exam Objectives</td>
<td>435</td>
</tr>
<tr>
<td>Self Test</td>
<td>436</td>
</tr>
<tr>
<td>Self Test Quick Answer Key</td>
<td>438</td>
</tr>
<tr>
<td>Appendix: Self test</td>
<td>441</td>
</tr>
<tr>
<td>Glossary</td>
<td>489</td>
</tr>
<tr>
<td>Index</td>
<td>525</td>
</tr>
</tbody>
</table>
Acknowledgments

I need to first thank my wife Melissa and my children Eric and Emma, for their love and patience while I wrote this book. Thank you to contributing authors and my friends Joshua Feldman and Seth Misenar.

Thank you to my teachers and mentors: thank you Miss Gilmore, for sending me on my way. Thank you Dave Curado and Beef Mazzola, for showing me the right way to do it. Thank you Stephen Northcutt, Alan Paller, Deb Jorgensen, Scott Weil, Eric Cole, Ed Skoudis, Johannes Ullrich, and many others from the SANS Institute, for showing me how to take it to the next level.

I would like to thank the supergroup of information security professionals who answered my last minute call, and collectively wrote the 500 questions comprising the two sets of online practice exams: Rodney Caudle, David Crafts, Bruce Diamond, Jason Fowler, Philip Keibler, Warren Mack, Eric Mattingly, Ron Reidy, Mike Saurbaugh, and Gary Whitsett.

Thank you to Michael Strickland for help with figures in Chapter 3. Thank you Rachel Roumeliotis and Matthew Cater of Syngress, for the support and dedication to this book.

Contributing author Seth Misenar writes the following: “I would like to thank my wife, Rachel, the love of my life, who showed continued patience, support, and strength when entertaining two young children throughout this writing process. I am grateful to my children, Jude and Hazel, who, at 3 and 0, were amazingly gracious when daddy had to write. And I count myself lucky to have such wonderful parents, Bob and Jeanine, who, as always, provided much of their time to ensure that my family was taken care of during this writing period.”
About the authors

LEAD AUTHOR

Eric Conrad (CISSP®, GIAC GSE, GPEN, GCIA, GCIA, GCFA, GAWN, GSEC and Security+) is a SANS Certified Instructor and is a partner with Backshore Communications, which provides information warfare, penetration testing, incident handling, and intrusion detection consulting services. Eric started his professional career in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care, in roles ranging from systems programmer to security engineer to HIPAA security officer and ISSO. He has taught over 1000 students in courses including SANS Management 414: CISSP®, Security 560: Network Penetration Testing and Ethical Hacking, Security 504 Hacker Techniques, Exploits & Incident Handling, and others.

Eric is a graduate of the SANS Technology Institute with a Master of Science degree in Information Security Engineering. Eric currently lives in Peaks Island, Maine with his family, Melissa, Eric and Emma.

CONTRIBUTING AUTHORS

Seth Misenar (CISSP®, GPEN, GCIA, GCIA, GCFA, GWAPT, GCWN, GSEC, MCSE, MCDBA) is a Certified Instructor with the SANS Institute and also serves as lead consultant for Jackson, Mississippi-based Context Security. Seth’s background includes security research, network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as a physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Seth teaches a variety of courses for the SANS Institute, including Security Essentials, Web Application Penetration Testing, Hacker Techniques, and the CISSP® course.

Seth is pursuing a Master of Science degree in Information Security Engineering from the SANS Technology Institute and holds a Bachelor of Science degree from Millsaps College. Seth resides in Jackson, Mississippi with his family, Rachel, Jude, and Hazel.
Joshua Feldman (CISSP®, NSA IAM) has supported the Department of Defense Information Systems Agency as a contractor working for SAIC, Inc. Since 2002, he was a subject matter expert and training developer for DISA’s cyber security mission. During his tenure, he contributed to the DoD 8500 series, specifically conducting research and authoring sections of the DoD 8570.01-M, also known as the DoD IA Workforce Improvement Program. He has taught well over 1000 DoD students through his “DoD IA Boot Camp” course. He is also a subject matter expert for the Web-based Information Assurance awareness training that every DoD user is required to take each year as part of their security awareness curriculum. He is a regular presenter and panel member at the Information Assurance Symposium, hosted by both DISA and NSA.

Before joining the support team at DoD/DISA, Joshua spent time as an IT Sec engineer working for the Department of State, Diplomatic Security. There, he travelled to embassies worldwide to conduct Tiger Team assessments of the security of each embassy. Joshua got his start in the IT Security field when he left his position teaching science for Montgomery County Public Schools, Maryland and went to work for NFR Security Software. At the time, NFR was one of the leading companies producing Network Intrusion Detection systems.

ABOUT THE TECHNICAL EDITOR

Kevin Riggins (CISSP®) has over 22 years of experience in Information Technology and has focused on Information Security since 1999. He has been a Certified Information Systems Security Professional since 2004 and currently works for a Fortune 500 financial service company where he leads a team of information security analysts responsible for internal consulting, risk assessments, and vendor security reviews. He writes about various information security topics on his blog, Infosec Ramblings (http://www.infosecramblings.com), his articles have been published in (IN)Secure magazine, and he is a frequent speaker at conference and industry association meetings.