

# CISSP<sup>®</sup> Study Guide



# CISSP<sup>®</sup> Study Guide

**Eric Conrad**

**Seth Misenar**

**Joshua Feldman**

Technical Editor

**Kevin Riggins**



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON  
NEW YORK • OXFORD • PARIS • SAN DIEGO  
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

**SYNGRESS<sup>®</sup>**

**Acquiring Editor: Rachel Roumeliotis**  
**Development Editor: Matthew Cater**  
**Project Manager: Andre Cuello**  
**Designer: Alisa Andreola**

Syngress is an imprint of Elsevier  
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

© 2010 Elsevier, Inc. All rights reserved.

CISSP® and (ISC)<sup>2</sup> are registered marks of the International Information Systems Security Certification Consortium, Inc. (ISC)<sup>2</sup>. No endorsement by or association with (ISC)<sup>2</sup> is expressed or implied by the use of the marks.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

#### Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

#### Library of Congress Cataloging-in-Publication Data

Conrad, Eric, 1967–

CISSP study guide / Eric Conrad, Seth Misenar, Joshua Feldman.

p. cm.

ISBN 978-1-59749-563-9

1. Electronic data processing personnel—Certification. 2. Computer networks—Examinations—Study guides. I. Misenar, Seth. II. Feldman, Joshua. III. Title.

QA76.3.C497 2010

004.6—dc22

2010018643

#### British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN: 978-1-59749-563-9

Printed in the United States of America

10 11 12 13 14 10 9 8 7 6 5 4 3 2 1

Working together to grow  
libraries in developing countries

[www.elsevier.com](http://www.elsevier.com) | [www.bookaid.org](http://www.bookaid.org) | [www.sabre.org](http://www.sabre.org)

ELSEVIER

BOOK AID  
International

Sabre Foundation

For information on all Syngress publications visit our website at [www.syngress.com](http://www.syngress.com)

# Contents

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

<b>CHAPTER 1 Introduction .....</b>	<b>1</b>
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

<b>CHAPTER 2 Domain 1: Information security governance and risk management .....</b>	<b>7</b>
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

	Security Policy and Related Documents .....	22
	Security Awareness and Training .....	24
	Roles and Responsibilities .....	25
	Compliance with Laws and Regulations .....	26
	Privacy .....	26
	Due Care and Due Diligence .....	26
	Best Practice .....	27
	Outsourcing and Offshoring.....	27
	Auditing and Control Frameworks .....	28
	Certification and Accreditation .....	30
	Ethics .....	31
	The (ISC) <sup>2</sup> © Code of Ethics .....	31
	Summary of Exam Objectives .....	32
	Self Test.....	32
	Self Test Quick Answer Key .....	34
<b>CHAPTER 3</b>	<b>Domain 2: Access control.....</b>	<b>37</b>
	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

Deterrent .....	52
Compensating .....	52
Comparing Access Controls.....	52
Authentication Methods .....	53
Type 1 Authentication: Something You Know.....	53
Type 2 Authentication: Something You Have.....	59
Type 3 Authentication: Something You Are .....	61
Someplace You Are .....	67
Access Control Technologies.....	67
Single Sign-On (SSO) .....	67
Kerberos.....	68
SESAME.....	72
Security Audit Logs .....	72
Types of Attackers .....	73
Hackers .....	73
Black Hats and White Hats.....	74
Script Kiddies .....	74
Outsiders .....	75
Insiders.....	76
Hacktivist.....	77
Bots and BotNets.....	77
Phishers and Spear Phishers.....	79
Assessing Access Control .....	79
Penetration Testing.....	82
Vulnerability Testing.....	84
Security Audits .....	84
Security Assessments .....	84
Summary of Exam Objectives .....	85
Self Test.....	85
Self Test Quick Answer Key.....	88
<b>CHAPTER 4 Domain 3: Cryptography .....</b>	<b>91</b>
Unique Terms and Definitions.....	91
Introduction.....	91
Cornerstone Cryptographic Concepts .....	91
Key Terms .....	92
Confidentiality, Integrity, Authentication, and Non-Repudiation.....	92
Confusion, Diffusion, Substitution, and Permutation .....	92
Cryptographic Strength .....	93
Monoalphabetic and Polyalphabetic Ciphers .....	93

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
<b>CHAPTER 5 Domain 4: Physical (Environmental) security.....</b>	<b>131</b>
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

System Defenses.....	146
Asset Tracking.....	146
Port Controls.....	146
Drive and Tape Encryption.....	146
Media Storage and Transportation.....	147
Media Cleaning and Destruction .....	147
Environmental Controls.....	149
Electricity.....	149
HVAC .....	151
Heat, Flame, and Smoke Detectors .....	152
Safety Training and Awareness .....	153
ABCD Fires and Suppression .....	154
Types of Fire Suppression Agents.....	156
Summary of Exam Objectives .....	160
Self Test.....	160
Self Test Quick Answer Key .....	163
<b>CHAPTER 6 Domain 5: Security architecture and design .....</b>	<b>165</b>
Unique Terms and Definitions.....	165
Introduction.....	165
Secure System Design Concepts.....	166
Layering.....	166
Abstraction.....	166
Security Domains .....	167
The Ring Model .....	167
Open and Closed Systems.....	168
Secure Hardware Architecture .....	168
The System Unit and Motherboard .....	168
The Computer Bus .....	169
The CPU .....	170
Memory.....	172
Memory Protection.....	174
Secure Operating System and Software Architecture.....	177
The Kernel.....	178
Users and File Permissions .....	178
Virtualization .....	181
Thin Clients .....	182
System Vulnerabilities, Threats, and Countermeasures.....	183
Emanations.....	183
Covert Channels .....	183
Buffer Overflows.....	184

TOCTOU/Race Conditions .....	185
Backdoors .....	185
Malicious Code (Malware) .....	186
Server-Side Attacks .....	187
Client-Side Attacks.....	188
Web Application Attacks .....	189
Mobile Device Attacks.....	190
Database Security .....	191
Countermeasures.....	193
Security Models.....	193
Reading Down and Writing Up.....	193
State Machine model.....	195
Bell-LaPadula model.....	195
Lattice-Based Access Controls .....	196
Integrity Models .....	197
Information Flow Model.....	198
Chinese Wall Model.....	199
Noninterference .....	199
Take-Grant .....	199
Access Control Matrix .....	200
Zachman Framework for Enterprise Architecture.....	200
Graham-Denning Model.....	200
Harrison-Ruzzo-Ullman Model.....	201
Modes of Operation.....	202
Evaluation Methods, Certification, and Accreditation.....	202
The Orange Book .....	203
ITSEC .....	204
The International Common Criteria.....	205
PCI-DSS.....	206
Certification and Accreditation.....	206
Summary of Exam Objectives .....	206
Self Test.....	207
Self Test Quick Answer Key.....	209
<b>CHAPTER 7 Domain 6: Business continuity and disaster</b>	
<b>recovery planning .....</b>	<b>211</b>
Unique Terms and Definitions.....	211
Introduction.....	211
BCP and DRP Overview and Process .....	212
Business Continuity Planning (BCP).....	212
Disaster Recovery Planning (DRP) .....	213

Relationship between BCP and DRP .....	213
Disasters or disruptive Events.....	214
The Disaster Recovery Process.....	221
Developing a BCP/DRP.....	223
Project Initiation .....	224
Scoping the Project .....	227
Assessing the Critical State.....	227
Conduct Business Impact Analysis (BIA).....	228
Identify Preventive Controls .....	232
Recovery Strategy .....	232
Related Plans .....	236
Plan Approval.....	241
Backups and Availability .....	241
Hardcopy Data.....	242
Electronic Backups.....	243
Software Escrow.....	245
DRP Testing, Training, and Awareness .....	245
DRP Testing .....	246
Training.....	248
Awareness.....	248
Continued BCP/DRP Maintenance .....	248
Change Management .....	248
BCP/DRP Mistakes .....	249
Specific BCP/DRP Frameworks .....	249
NIST SP 800-34 .....	249
ISO/IEC-27031 .....	250
BS-25999 .....	250
BCI.....	251
Summary of Exam Objectives .....	251
Self Test.....	251
Self Test Quick Answer Key .....	253
<b>CHAPTER 8 Domain 7: Telecommunications and network security .....</b>	<b>255</b>
Unique Terms and Definitions.....	255
Introduction.....	255
Network Architecture and Design .....	256
Network Defense-in-Depth .....	256
Fundamental Network Concepts .....	256
The OSI Model.....	259
The TCP/IP Model .....	261
Encapsulation.....	262

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
<b>CHAPTER 9 Domain 8: Application development security .....</b>	<b>329</b>
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

Top-Down versus Bottom-Up Programming.....	333
Types of Publicly Released Software.....	334
Application Development Methods .....	335
Waterfall Model.....	336
Sashimi Model.....	337
Agile Software Development.....	339
Spiral.....	340
Rapid Application Development (RAD) .....	341
Prototyping.....	341
SDLC .....	342
Software Escrow.....	346
Object-Orientated Design and Programming .....	346
Object-Oriented Programming (OOP) .....	346
Object Request Brokers.....	349
Object-Oriented Analysis (OOA) and Object-Oriented Design (OOD).....	351
Software Vulnerabilities, Testing, and Assurance .....	351
Software Vulnerabilities.....	352
Software Testing Methods .....	353
Disclosure .....	355
Software Capability Maturity Model (CMM).....	356
Databases .....	356
Types of Databases .....	357
Database Integrity.....	361
Database Replication and Shadowing.....	361
Data Warehousing and Data Mining .....	362
Artificial Intelligence .....	362
Expert Systems.....	362
Artificial Neural Networks.....	363
Bayesian Filtering.....	364
Genetic Algorithms and Programming .....	365
Summary of Exam Objectives .....	365
Self Test.....	366
Self Test Quick Answer Key.....	368
<b>CHAPTER 10 Domain 9: Operations security .....</b>	<b>371</b>
Unique Terms and Definitions.....	371
Introduction.....	371
Administrative Security.....	372
Administrative Personnel Controls .....	372
Privilege Monitoring .....	375

Sensitive Information/Media Security .....	376
Sensitive Information .....	376
Asset Management .....	378
Configuration Management.....	379
Change Management.....	381
Continuity of Operations.....	383
Service Level Agreements (SLA).....	383
Fault Tolerance.....	384
Incident Response Management .....	390
Methodology.....	391
Types of attacks.....	393
Summary of Exam Objectives .....	398
Self Test.....	400
Self Test Quick Answer Key.....	403

## **CHAPTER 11 Domain 10: Legal regulations, investigations, and**

<b>compliance.....</b>	<b>405</b>
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

Reasonable Searches .....	426
Entrapment and enticement.....	428
Important Laws and Regulations .....	429
U.S. Computer Fraud and Abuse Act.....	430
USA PATRIOT Act .....	431
HIPAA .....	431
United States Breach Notification Laws .....	432
Ethics .....	433
Computer Ethics Institute.....	433
IAB's Ethics and the Internet .....	434
The (ISC) <sup>2</sup> © Code of Ethics .....	434
Summary of Exam Objectives .....	435
Self Test.....	436
Self Test Quick Answer Key .....	438
<b>Appendix: Self test.....</b>	<b>441</b>
<b>Glossary .....</b>	<b>489</b>
<b>Index.....</b>	<b>525</b>



# 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<sup>®</sup>, GIAC GSE, GPEN, GCIH, 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<sup>®</sup>, 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<sup>®</sup>, GPEN, GCIH, 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<sup>®</sup> 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<sup>®</sup>, 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<sup>®</sup>) 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.