

▲Praise for CISSP® All-in-One Exam Guide

Fernando's latest update to the CISSP All-In-One Exam Guide continues the tradition

started in past collaborations with Shon Harris of breaking down key concepts and critical skills in a way that prepares the reader for the exam. Once again the material proves to

be not only a vital asset to exam preparation but a valued resource reference for use well

after the exam has been passed.

Stefanie Keuser, CISSP,

Chief Information Officer,

Military Officers Association of America

The CISSP All-in-One Exam Guide is the only book one needs to pass the CISSP exam.

Fernando Maymí is not just an author, he is a leader in the cybersecurity industry. His

insight, knowledge, and expertise is reflected in the content provided in this book. The

book will not only give you what you need to pass the exam, it can also be used to help

you further your career in cybersecurity.

Marc Coady, CISSP,

Compliance Analyst,

Costco Wholesale

A must-have reference for any cyber security practitioner, this book provides invaluable

practical knowledge on the increasingly complex universe of security concepts, controls,

and best practices necessary to do business in today's world.

Steve Zalewski,

Former Chief Information Security Officer,

Levi Strauss & Co.

Shon Harris put the CISSP certification on the map with this golden bible of the CISSP.

Fernando Maymí carries that legacy forward beautifully with clarity, accuracy, and

balance. I am sure that Shon would be proud.

David R. Miller, CISSP, CCSP, GIAC GISP GSEC GISF,

PCI QSA, LPT, ECSA, CEH, CWNA, CCNA, SME, MCT,

MCIT Pro EA, MCSE: Security, CNE, Security+, etc.

▲An excellent reference. Written clearly and concisely, this book is invaluable to students,

educators, and practitioners alike.

Dr. Joe Adams,

Founder and Executive Director,

Michigan Cyber Range

A lucid, enlightening, and comprehensive tour de force through the breadth of cyber

security. Maymí and Harris are masters of the craft.

Dr. Greg Conti,

Founder,

Kopidion LLC

I wish I found this book earlier in my career. It certainly was the single tool

I used to pass the CISSP exam, but more importantly it has taught me about security from many aspects I did not even comprehend previously. I think the knowledge that I gained from this book is going to help me in many years to come. Terrific book and resource!

Janet Robinson,  
Chief Security Officer

## ♣ALL IN ONE

CISSP

®

## EXAM GUIDE

### ♣ABOUT THE AUTHORS

Fernando Maymí, PhD, CISSP, is a security practitioner with over 25 years' experience in the field. He is currently Vice President of Training at IronNet Cybersecurity, where, besides developing cyber talent for the company, its partners, and customers, he has led teams providing strategic consultancy, security assessments, red teaming, and cybersecurity exercises around the world. Previously, he led advanced research and development projects at the intersection of artificial intelligence and cybersecurity, stood up the U.S. Army's think tank for strategic cybersecurity issues, and was a West Point faculty member for over 12 years. Fernando worked closely with

Shon Harris, advising her on a multitude of projects, including the sixth edition of the

CISSP All-in-One Exam Guide.

Shon Harris, CISSP, was the founder and CEO of Shon Harris Security LLC and Logical Security LLC, a security consultant, a former engineer in the Air Force's Information Warfare unit, an instructor, and an author. Shon owned and ran her own

training and consulting companies for 13 years prior to her death in 2014. She consulted

with Fortune 100 corporations and government agencies on extensive security issues. She

authored three best-selling CISSP books, was a contributing author to Gray Hat Hacking:

The Ethical Hacker's Handbook and Security Information and Event Management (SIEM)

Implementation, and a technical editor for Information Security Magazine.

### About the Contributor/Technical Editor

Bobby E. Rogers is an information security engineer working as a contractor for Department of Defense agencies, helping to secure, certify, and accredit their information systems. His duties include information system security engineering, risk management, and

certification and accreditation efforts. He retired after 21 years in the U.S. Air Force,

serving as a network security engineer and instructor, and has secured networks

all over  
the world. Bobby has a master's degree in information assurance (IA) and is  
pursuing a  
doctoral degree in cybersecurity from Capitol Technology University in Maryland.  
His  
many certifications include CISSP-ISSEP, CEH, and MCSE: Security, as well as the  
CompTIA A+, Network+, Security+, and Mobility+ certifications.

♣ALL IN ONE

CISSP

®

EXAM GUIDE  
Ninth Edition

Fernando Maymí  
Shon Harris

New York Chicago San Francisco  
Athens London Madrid Mexico City  
Milan New Delhi Singapore Sydney Toronto

McGraw Hill is an independent entity from (ISC)<sup>2</sup>® and is not affiliated with  
(ISC)<sup>2</sup> in any manner. This study/training  
guide and/or material is not sponsored by, endorsed by, or affiliated with  
(ISC)<sup>2</sup> in any manner. This publication and  
accompanying media may be used in assisting students to prepare for the CISSP  
exam. Neither (ISC)<sup>2</sup> nor McGraw Hill  
warrants that use of this publication and accompanying media will ensure passing  
any exam. (ISC)<sup>2</sup>®, CISSP®, CAP®,  
ISSAP®, ISSEP®, ISSMP®, SSCP® and CBK® are trademarks or registered trademarks  
of (ISC)<sup>2</sup> in the United States and  
certain other countries. All other trademarks are trademarks of their respective  
owners.

♣Copyright © 2022 by McGraw Hill. All rights reserved. Except as permitted under  
the United States Copyright Act of 1976,  
no part of this publication may be reproduced or distributed in any form or by  
any means, or stored in a database or retrieval  
system, without the prior written permission of the publisher.

ISBN: 978-1-26-046736-9

MHID:

1-26-046736-8

The material in this eBook also appears in the print version of this title:

ISBN: 978-1-26-046737-6,

MHID: 1-26-046737-6.

eBook conversion by codeMantra

Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a  
trademark symbol after every occurrence of a  
trademarked name, we use names in an editorial fashion only, and to the benefit  
of the trademark owner, with no intention of

infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at [www.mhprofessional.com](http://www.mhprofessional.com).

Information has been obtained by McGraw Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw Hill, or others, McGraw Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

#### TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent.

You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your

right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." MCGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES

OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED

FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK

VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in

the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education

nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work

or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work.

Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect,

incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if

any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause

whatsoever whether such claim or cause arises in contract, tort or otherwise.

♠We dedicate this book to all those who have served others selflessly.

♠This page intentionally left blank

▲CONTENTS AT A GLANCE

Part I

Security and Risk Management

Chapter 1

Cybersecurity Governance . . . . . 3

Chapter 2

Risk Management . . . . . 53

Chapter 3

Compliance . . . . . 125

Chapter 4

Frameworks . . . . . 171

Part II

Asset Security

Chapter 5

Assets . . . . . 213

Chapter 6

Data Security. . . . . 253

Part III

Security Architecture and Engineering

Chapter 7

System Architectures. . . . . 283

Chapter 8

Cryptology . . . . . 317

Chapter 9

Security Architectures . . . . . 385

Chapter 10

Site and Facility Security . . . . . 417

Part IV

Communication and Network Security

Chapter 11

Networking Fundamentals . . . . . 469

Chapter 12

Wireless Networking . . . . . 559

Chapter 13

Securing the Network . . . . . 597

Chapter 14

Network Components . . . . . 643

Chapter 15

Secure Communications Channels . . . . . 681

Part V

Identity and Access Management

Chapter 16

Identity and Access Fundamentals . . . . . 715

Chapter 17

Managing Identities and Access . . . . . 765

## ▲CISSP All-in-One Exam Guide

x

### Part VI

#### Security Assessment and Testing

##### Chapter 18

Security Assessments . . . . .	813
--------------------------------	-----

##### Chapter 19

Measuring Security . . . . .	851
------------------------------	-----

### Part VII Security Operations

##### Chapter 20

Managing Security Operations . . . . .	885
--	-----

##### Chapter 21

Security Operations . . . . .	939
-------------------------------	-----

##### Chapter 22

Security Incidents . . . . .	989
------------------------------	-----

##### Chapter 23

Disasters . . . . .	1029
---------------------	------

### Part VIII Software Development Security

##### Chapter 24

Software Development . . . . .	1079
--------------------------------	------

##### Chapter 25

Secure Software . . . . .	1117
---------------------------	------

Appendix A Comprehensive Questions . . . . .	1155
--	------

Appendix B Objective Map . . . . .	1209
------------------------------------	------

Appendix C About the Online Content . . . . .	
---	--

.....	1225
Glossary .....	
.....	1231
Index. ....	
.....	1253

## ▲CONTENTS

From the Author .....	
.....	xxix
Acknowledgments .....	
.....	xxxiii
Why Become a CISSP? .....	
.....	xxxv

## Part I

### Chapter 1

#### Security and Risk Management

Cybersecurity Governance .....	
.....	
Fundamental Cybersecurity Concepts and Terms .....	
Confidentiality .....	
.....	
Integrity .....	
.....	
Availability .....	
.....	
Authenticity .....	
.....	
Nonrepudiation .....	
.....	
Balanced Security .....	
.....	
Other Security Terms .....	
.....	
Security Governance Principles .....	
.....	
Aligning Security to Business Strategy .....	
Organizational Processes .....	
Organizational Roles and Responsibilities .....	
Security Policies, Standards, Procedures, and Guidelines .....	
Security Policy .....	
.....	
Standards .....	
.....	
Baselines .....	
.....	
Guidelines .....	
.....	
Procedures .....	
.....	
Implementation .....	
.....	
Personnel Security .....	



.....	
Candidate Screening and Hiring . . . . .	
Employment Agreements and Policies . . . . .	
Onboarding, Transfers, and Termination Processes . . . . .	
Vendors, Consultants, and Contractors . . . . .	
Compliance Policies . . . . .	
.	
Privacy Policies . . . . .	
....	
Security Awareness, Education, and Training Programs . . . . .	
Degree or Certification? . . . . .	
.	
Methods and Techniques to Present	
Awareness and Training . . . . .	

3
4
5
5
6
6
6
7
8
10
13
17
18
25
27
29
31
32
32
32
33
35
36
37
39
39
40
40
40
41

xi

♣CISSP All-in-One Exam Guide

xii

Chapter 2

Periodic Content Reviews . . . . .	
Program Effectiveness Evaluation . . . . .	
Professional Ethics . . . . .	
. . . . .	
(ISC)2 Code of Professional Ethics . . . . .	
Organizational Code of Ethics . . . . .	
The Computer Ethics Institute . . . . .	
Chapter Review . . . . .	
. . . . .	
Quick Review . . . . .	
. . . . .	
Questions . . . . .	
. . . . .	
Answers . . . . .	
. . . . .	

43  
43  
44  
44  
45  
45  
46  
46  
48  
51

Risk Management . . . . .	
. . . . .	
Risk Management Concepts . . . . .	
. . . . .	
Holistic Risk Management . . . . .	
Information Systems Risk Management Policy . . . . .	
The Risk Management Team . . . . .	
The Risk Management Process . . . . .	
Overview of Vulnerabilities and Threats . . . . .	
Identifying Threats and Vulnerabilities . . . . .	
Assessing Risks . . . . .	
. . . . .	
Asset Valuation . . . . .	
. . . . .	
Risk Assessment Teams . . . . .	
Methodologies for Risk Assessment . . . . .	
Risk Analysis Approaches . . . . .	
Qualitative Risk Analysis . . . . .	
. . . . .	
Responding to Risks . . . . .	
. . . . .	
Total Risk vs. Residual Risk . . . . .	
Countermeasure Selection and Implementation . . . . .	
Types of Controls . . . . .	
. . . . .	
Control Assessments . . . . .	
. . . . .	

Monitoring Risks . . . . .	
Effectiveness Monitoring . . . . .	
Change Monitoring . . . . .	
Compliance Monitoring . . . . .	
Risk Reporting . . . . .	
Continuous Improvement . . . . .	
Supply Chain Risk Management . . . . .	
Upstream and Downstream Suppliers . . . . .	
Risks Associated with Hardware, Software, and Services . . . . .	
Other Third-Party Risks . . . . .	
Minimum Security Requirements . . . . .	
Service Level Agreements . . . . .	
Business Continuity . . . . .	
Standards and Best Practices . . . . .	
Making BCM Part of the Enterprise Security Program . . . . .	
Business Impact Analysis . . . . .	

53
53
54
56
56
57
58
62
63
65
66
67
72
76
79
81
81
83
88
91
91
92
93
94
95
96
98
98
99
100
101
101

104  
106  
108

## ▲Contents

xiii

## Chapter 3

## Chapter 4

Chapter Review . . . . .	.
Quick Review . . . . .	.
Questions . . . . .	.
Answers . . . . .	.
116	
116	
118	
121	
Compliance . . . . .	.
Laws and Regulations . . . . .	.
Types of Legal Systems . . . . .	.
Common Law Revisited . . . . .	.
Cybercrimes and Data Breaches . . . . .	.
Complexities in Cybercrime . . . . .	.
The Evolution of Attacks . . . . .	.
International Issues . . . . .	.
Data Breaches . . . . .	.
Import/Export Controls . . . . .	.
Transborder Data Flow . . . . .	.
Privacy . . . . .	.
Licensing and Intellectual Property Requirements . . . . .	.
Trade Secret . . . . .	.
Copyright . . . . .	.
Trademark . . . . .	.
Patent . . . . .	.
Internal Protection of Intellectual Property . . . . .	.

Software Piracy . . . . .

    . . . . .

Compliance Requirements . . . . .

    . . . . .

Contractual, Legal, Industry Standards,  
and Regulatory Requirements . . . . .

Privacy Requirements . . . . .

Liability and Its Ramifications . . . . .

Requirements for Investigations . . . . .

    . . . . .

Administrative . . . . .

    . . . . .

Criminal . . . . .

    . . . . .

Civil . . . . .

    . . . . .

Regulatory . . . . .

    . . . . .

Chapter Review . . . . .

    . . . . .

Quick Review . . . . .

    . . . . .

Questions . . . . .

    . . . . .

Answers . . . . .

    . . . . .

125

125

126

129

130

132

134

138

139

145

146

147

147

148

149

150

151

152

153

155

Frameworks . . . . .

    . . . . .

Overview of Frameworks . . . . .

    . . . . .

Risk Frameworks . . . . .

    . . . . .

NIST RMF . . . . .	171
ISO/IEC 27005 . . . . .	171
OCTAVE . . . . .	173
FAIR . . . . .	173
	177
	178
	179

171  
171  
173  
173  
177  
178  
179

156  
158  
158  
161  
161  
162  
162  
162  
162  
163  
165  
168

## ▲CISSP All-in-One Exam Guide

xiv	
Information Security Frameworks . . . . .	156
Security Program Frameworks . . . . .	158
Security Control Frameworks . . . . .	158
Enterprise Architecture Frameworks . . . . .	161
Why Do We Need Enterprise Architecture Frameworks? . . . .	161
Zachman Framework . . . . .	162
The Open Group Architecture Framework . . . . .	162
Military-Oriented Architecture Frameworks . . . . .	162
Other Frameworks . . . . .	163
ITIL . . . . .	165
Six Sigma . . . . .	168
Capability Maturity Model . . . . .	
Putting It All Together . . . . .	
Chapter Review . . . . .	

Quick Review . . . . .

..

Questions . . . . .

.. . . .

Answers . . . . .

.. . . .

Part II

Chapter 5

179

180

183

189

191

192

194

195

196

196

197

197

199

203

203

205

208

Asset Security

Assets . . . . .

.. . . .

Information and Assets . . . . .

.. . . .

Identification . . . . .

.. . . .

Classification . . . . .

.. . . .

Physical Security Considerations . . . . .

.. . . .

Protecting Mobile Devices . . . . .

Paper Records . . . . .

.. . . .

Safes . . . . .

.. . . .

Managing the Life Cycle of Assets . . . . .

.. . . .

Ownership . . . . .

.. . . .

Inventories . . . . .

.. . . .

Secure Provisioning . . . . .

.. . . .

Asset Retention . . . . .

.. . . .

Data Life Cycle . . . . .  
Data Acquisition . . . . .  
Data Storage . . . . .  
Data Use . . . . .  
Data Sharing . . . . .  
Data Archival . . . . .  
Data Destruction . . . . .  
Data Roles . . . . .  
Chapter Review . . . . .  
Quick Review . . . . .  
Questions . . . . .  
Answers . . . . .

213  
214  
214  
215  
220  
220  
221  
221  
222  
223  
224  
227  
228  
230  
230  
232  
237  
238  
239  
240  
244  
245  
245  
247  
250



## Chapter 6

### Part III

## Chapter 7

Data Security . . . . .	.
. . . . .	.
Data Security Controls . . . . .	.
. . . . .	.
Data States . . . . .	.
. . . . .	.
Standards . . . . .	.
. . . . .	.
Scoping and Tailoring . . . . .	.
.	.
Data Protection Methods . . . . .	.
. . . . .	.
Digital Asset Management . . . . .	.
Digital Rights Management . . . . .	.
Data Loss Prevention . . . . .	.
.	.
Cloud Access Security Broker . . . . .	.
Chapter Review . . . . .	.
. . . . .	.
Quick Review . . . . .	.
.	.
Questions . . . . .	.
. . . . .	.
Answers . . . . .	.
. . . . .	.

253

253

254

258

258

258

261

263

265

275

276

276

277

279

## Security Architecture and Engineering

System Architectures . . . . .	.
. . . . .	.
General System Architectures . . . . .	.
. . . . .	.
Client-Based Systems . . . . .	.
.	.
Server-Based Systems . . . . .	.

.	
Database Systems . . . . .	
.	
High-Performance Computing Systems . . . . .	
Industrial Control Systems . . . . .	
. . . . .	
Devices . . . . .	
. . . . .	
Distributed Control System . . . . .	
Supervisory Control and Data Acquisition . . . . .	
ICS Security . . . . .	
. . . . .	
Virtualized Systems . . . . .	
. . . . .	
Virtual Machines . . . . .	
. . . . .	
Containerization . . . . .	
. . . . .	
Microservices . . . . .	
. . . . .	
Serverless . . . . .	
. . . . .	
Cloud-Based Systems . . . . .	
. . . . .	
Software as a Service . . . . .	
. . . . .	
Platform as a Service . . . . .	
. . . . .	
Infrastructure as a Service . . . . .	
. . . . .	
Everything as a Service . . . . .	
. . . . .	
Cloud Deployment Models . . . . .	
Pervasive Systems . . . . .	
. . . . .	
Embedded Systems . . . . .	
Internet of Things . . . . .	
. . . . .	
Distributed Systems . . . . .	
. . . . .	
Edge Computing Systems . . . . .	

283  
 283  
 284  
 284  
 285  
 288  
 289  
 291  
 293  
 294  
 294  
 296

296  
298  
299  
299  
301  
302  
303  
304  
304  
305  
305  
306  
306  
307  
308

#### ▲CISSP All-in-One Exam Guide

xvi	
Chapter Review . . . . .	
. . . . .	
Quick Review . . . . .	
. . . . .	
Questions . . . . .	
. . . . .	
Answers . . . . .	
. . . . .	

310  
310  
311  
314

#### Chapter 8

Cryptology . . . . .	
. . . . .	
The History of Cryptography . . . . .	
. . . . .	
Cryptography Definitions and Concepts . . . . .	
Cryptosystems . . . . .	
. . . . .	
Kerckhoffs' Principle . . . . .	
. . . . .	
The Strength of the Cryptosystem . . . . .	
One-Time Pad . . . . .	
. . . . .	
Cryptographic Life Cycle . . . . .	
Cryptographic Methods . . . . .	
. . . . .	
Symmetric Key Cryptography . . . . .	
Asymmetric Key Cryptography . . . . .	
Elliptic Curve Cryptography . . . . .	
Quantum Cryptography . . . . .	

Hybrid Encryption Methods . . . . .	
Integrity . . . . .	
. . . . .	
Hashing Functions . . . . .	
.	
Message Integrity Verification . . . . .	
Public Key Infrastructure . . . . .	
. . . . .	
Digital Certificates . . . . .	
. . . . .	
Certificate Authorities . . . . .	
. . . . .	
Registration Authorities . . . . .	
.	
PKI Steps . . . . .	
. . . . .	
Key Management . . . . .	
Attacks Against Cryptography . . . . .	
. . . . .	
Key and Algorithm Attacks . . . . .	
Implementation Attacks . . . . .	
Other Attacks . . . . .	
. . . . .	
Chapter Review . . . . .	
. . . . .	
Quick Review . . . . .	
. . . . .	
Questions . . . . .	
. . . . .	
Answers . . . . .	
. . . . .	

317  
 317  
 321  
 323  
 324  
 325  
 325  
 328  
 328  
 329  
 335  
 342  
 344  
 346  
 351  
 351  
 354  
 359  
 359  
 360  
 362  
 362

364  
367  
367  
370  
372  
375  
376  
379  
381

## Chapter 9

Security Architectures . . . . .	.
Threat Modeling . . . . .	.
Attack Trees . . . . .	.
STRIDE . . . . .	.
The Lockheed Martin Cyber Kill Chain . . . . .	.
The MITRE ATT&CK Framework . . . . .	.
Why Bother with Threat Modeling . . . . .	.

385  
385  
386  
387  
387  
389  
389

## ▲Contents

xvii	
Secure Design Principles . . . . .	.
Defense in Depth . . . . .	.
Zero Trust . . . . .	.
Trust But Verify . . . . .	.
Shared Responsibility . . . . .	.
Separation of Duties . . . . .	.
Least Privilege . . . . .	.
Keep It Simple . . . . .	.
Secure Defaults . . . . .	.
Fail Securely . . . . .	.

. . . . .	
Privacy by Design . . . . .	
. . .	
Security Models . . . . .	
. . . . .	
Bell-LaPadula Model . . . . .	
.	
Biba Model . . . . .	
. . . . .	
Clark-Wilson Model . . . . .	
Noninterference Model . . . . .	
Brewer and Nash Model . . . . .	
Graham-Denning Model . . . . .	
Harrison-Ruzzo-Ullman Model . . . . .	
Security Requirements . . . . .	
. . . . .	
Security Capabilities of Information Systems . . . . .	
Trusted Platform Module . . . . .	
Hardware Security Module . . . . .	
Self-Encrypting Drive . . . . .	
.	
Bus Encryption . . . . .	
. . .	
Secure Processing . . . . .	
. . . . .	
Chapter Review . . . . .	
. . . . .	
Quick Review . . . . .	
. . .	
Questions . . . . .	
. . . . .	
Answers . . . . .	
. . . . .	

390  
 390  
 392  
 392  
 392  
 393  
 394  
 395  
 396  
 396  
 397  
 397  
 398  
 399  
 400  
 400  
 402  
 402  
 402  
 404

404  
404  
406  
407  
407  
408  
411  
412  
413  
415

Chapter 10 Site and Facility Security . . . . .	
. . . . .	
Site and Facility Design . . . . .	
. . . . .	
Security Principles . . . . .	
. . . . .	
The Site Planning Process . . . . .	
Crime Prevention Through Environmental Design . . . . .	
Designing a Physical Security Program . . . . .	
Site and Facility Controls . . . . .	
. . . . .	
Work Area Security . . . . .	
. . . . .	
Data Processing Facilities . . . . .	
. . . . .	
Distribution Facilities . . . . .	
. . . . .	
Storage Facilities . . . . .	
. . . . .	
Utilities . . . . .	
. . . . .	
Fire Safety . . . . .	
. . . . .	
Environmental Issues . . . . .	
. . . . .	

417  
417  
418  
423  
427  
433  
441  
441  
443  
446  
447  
448  
454  
461

xviii

Chapter Review . . . . .	.
Quick Review . . . . .	.
Questions . . . . .	.
Answers . . . . .	.

## Part IV

461  
461  
463  
465

## Communication and Network Security

Chapter 11 Networking Fundamentals . . . . .	.
Data Communications Foundations . . . . .	.
Network Reference Models . . . . .	.
Protocols . . . . .	.
Application Layer . . . . .	.
Presentation Layer . . . . .	.
Session Layer . . . . .	.
Transport Layer . . . . .	.
Network Layer . . . . .	.
Data Link Layer . . . . .	.
Physical Layer . . . . .	.
Functions and Protocols in the OSI Model . . . . .	.
Tying the Layers Together . . . . .	.
Local Area Networks . . . . .	.
Network Topology . . . . .	.
Medium Access Control Mechanisms . . . . .	.
Layer 2 Protocols . . . . .	.
Transmission Methods . . . . .	.
Layer 2 Security Standards . . . . .	.
Internet Protocol Networking . . . . .	.
TCP . . . . .	.



IP Addressing . . . . .	
. . . . .	
IPv6 . . . . .	
. . . . .	
Address Resolution Protocol . . . . .	
Dynamic Host Configuration Protocol . . . . .	
Internet Control Message Protocol . . . . .	
Simple Network Management Protocol . . . . .	
Domain Name Service . . . . .	
Network Address Translation . . . . .	
Routing Protocols . . . . .	
. . . . .	
Intranets and Extranets . . . . .	
. . . . .	
Metropolitan Area Networks . . . . .	
. . . . .	
Metro Ethernet . . . . .	
. . . . .	
Wide Area Networks . . . . .	
. . . . .	
Dedicated Links . . . . .	
. . . . .	
WAN Technologies . . . . .	

469

469

470

471

474

475

477

479

480

480

483

483

485

487

487

489

494

499

500

502

503

510

512

515

517

520

522

524

531

533

537  
538  
539  
540  
541  
543

## ▲Contents

xix

Chapter Review . . . . .	.
Quick Review . . . . .	.
Questions . . . . .	.
Answers . . . . .	.

552  
553  
555  
557

Chapter 12 Wireless Networking . . . . .	.
Wireless Communications Techniques . . . . .	.
Spread Spectrum . . . . .	.
Orthogonal Frequency Division Multiplexing . . . . .	.
Wireless Networking Fundamentals . . . . .	.
WLAN Components . . . . .	.
WLAN Standards . . . . .	.
Other Wireless Network Standards . . . . .	.
Other Important Standards . . . . .	.
Evolution of WLAN Security . . . . .	.
802.11 . . . . .	.
802.11i . . . . .	.
802.11w . . . . .	.
WPA3 . . . . .	.
802.1X . . . . .	.
Best Practices for Securing WLANs . . . . .	.
Mobile Wireless Communication . . . . .	.
Multiple Access Technologies . . . . .	.
Generations of Mobile Wireless . . . . .	.
Satellites . . . . .	.

Chapter Review . . . . .	559
Quick Review . . . . .	559
Questions . . . . .	561
Answers . . . . .	563

559  
 559  
 561  
 563  
 564  
 564  
 565  
 568  
 573  
 574  
 575  
 576  
 578  
 578  
 579  
 582  
 582  
 584  
 585  
 588  
 590  
 590  
 592  
 594

Chapter 13 Securing the Network . . . . .	594
Applying Secure Design Principles to Network Architectures . . . . .	594
Secure Networking . . . . .	594
Link Encryption vs. End-to-End Encryption . . . . .	594
TLS . . . . .	594
VPN . . . . .	594
Secure Protocols . . . . .	594
Web Services . . . . .	594
Domain Name System . . . . .	594
Electronic Mail . . . . .	594
Multilayer Protocols . . . . .	594

Distributed Network Protocol 3 . . . . .	
Controller Area Network Bus . . . . .	
Modbus . . . . .	
. . . . .	

597  
597  
599  
600  
602  
605  
611  
611  
616  
621  
626  
626  
627  
627

#### ▲CISSP All-in-One Exam Guide

xx	
Converged Protocols . . . . .	
. . . . .	
Encapsulation . . . . .	
. . . . .	
Fiber Channel over Ethernet . . . . .	
Internet Small Computer Systems Interface . . . . .	
Network Segmentation . . . . .	
. . . . .	
VLANs . . . . .	
. . . . .	
Virtual eXtensible Local Area Network . . . . .	
Software-Defined Networks . . . . .	
Software-Defined Wide Area Network . . . . .	
Chapter Review . . . . .	
. . . . .	
Quick Review . . . . .	
. . . . .	
Questions . . . . .	
. . . . .	
Answers . . . . .	
. . . . .	

627  
628  
628  
629  
629  
630  
632  
632  
635

635  
636  
638  
640

Chapter 14 Network Components . . . . .	.
Transmission Media . . . . .	.
Types of Transmission . . . . .	.
Cabling . . . . .	.
Bandwidth and Throughput . . . . .	.
Network Devices . . . . .	.
Repeaters . . . . .	.
Bridges . . . . .	.
Switches . . . . .	.
Routers . . . . .	.
Gateways . . . . .	.
Proxy Servers . . . . .	.
PBXs . . . . .	.
Network Access Control Devices . . . . .	.
Network Diagramming . . . . .	.
Operation of Hardware . . . . .	.
Endpoint Security . . . . .	.
Content Distribution Networks . . . . .	.
Chapter Review . . . . .	.
Quick Review . . . . .	.
Questions . . . . .	.
Answers . . . . .	.

643  
643  
644  
648  
654  
655  
655  
656

657  
660  
662  
663  
665  
667  
668  
670  
673  
674  
674  
675  
677  
678

Chapter 15 Secure Communications Channels . . . . .	
. . . . .	
Voice Communications . . . . .	
. . . . .	
Public Switched Telephone Network . . . . .	
DSL . . . . .	
. . . . .	
ISDN . . . . .	
. . . . .	
Cable Modems . . . . .	
. . . . .	
IP Telephony . . . . .	
. . . . .	

681  
682  
682  
683  
685  
686  
687

## ▲Contents

xxi	
Multimedia Collaboration . . . . .	
. . . . .	
Meeting Applications . . . . .	
. . . . .	
Unified Communications . . . . .	
Remote Access . . . . .	
. . . . .	
VPN . . . . .	
. . . . .	
Desktop Virtualization . . . . .	
Secure Shell . . . . .	
. . . . .	
Data Communications . . . . .	
. . . . .	

Network Sockets . . . . .

..

Remote Procedure Calls . . . . .

Virtualized Networks . . . . .

..

Third-Party Connectivity . . . . .

..

Chapter Review . . . . .

..

Quick Review . . . . .

..

Questions . . . . .

..

Answers . . . . .

..

Part V

693

694

695

696

697

699

701

702

703

703

704

705

707

707

709

711

Identity and Access Management

Chapter 16 Identity and Access Fundamentals . . . . .

..

Identification, Authentication, Authorization, and Accountability . . . .

Identification and Authentication . . . . .

Knowledge-Based Authentication . . . . .

Biometric Authentication . . . . .

Ownership-Based Authentication . . . . .

Credential Management . . . . .

..

Password Managers . . . . .

.

Password Synchronization . . . . .

Self-Service Password Reset . . . . .

Assisted Password Reset . . . . .

.

Just-in-Time Access . . . . .

..

Registration and Proofing of Identity . . . . .	
Profile Update . . . . .	
. . . . .	
Session Management . . . . .	
Accountability . . . . .	
. . . . .	
Identity Management . . . . .	
. . . . .	
Directory Services . . . . .	
. . . . .	
Directories' Role in Identity Management . . . . .	
Single Sign-On . . . . .	
. . . . .	
Federated Identity Management . . . . .	
Federated Identity with a Third-Party Service . . . . .	
Integration Issues . . . . .	
. . . . .	
On-Premise . . . . .	
. . . . .	
Cloud . . . . .	
. . . . .	
Hybrid . . . . .	
. . . . .	

715  
715  
718  
720  
723  
729  
736  
736  
737  
737  
738  
738  
738  
740  
740  
741  
745  
747  
748  
750  
752  
754  
754  
755  
756  
756



Chapter Review . . . . .	756
Quick Review . . . . .	757
Questions . . . . .	759
Answers . . . . .	762
Chapter 17 Managing Identities and Access . . . . .	
Authorization Mechanisms . . . . .	
Discretionary Access Control . . . . .	
Mandatory Access Control . . . . .	
Role-Based Access Control . . . . .	
Rule-Based Access Control . . . . .	
Attribute-Based Access Control . . . . .	
Risk-Based Access Control . . . . .	
Implementing Authentication and Authorization Systems . . . . .	
Access Control and Markup Languages . . . . .	
OAuth . . . . .	
OpenID Connect . . . . .	
Kerberos . . . . .	
Remote Access Control Technologies . . . . .	
Managing the Identity and Access Provisioning Life Cycle . . . . .	
Provisioning . . . . .	
Access Control . . . . .	
Compliance . . . . .	
Configuration Management . . . . .	
Deprovisioning . . . . .	
Controlling Physical and Logical Access . . . . .	
Information Access Control . . . . .	
System and Application Access Control . . . . .	
Access Control to Devices . . . . .	
Facilities Access Control . . . . .	
Chapter Review . . . . .	
Quick Review . . . . .	
Questions . . . . .	

Answers . . . . .	
-------------------	--

765
765
766
768
771
774
774
775
776
776
782
783
784
789
795
796
796
796
799
800
801
801
802
802
802
804
804
805
808

## Part VI

### Security Assessment and Testing

Chapter 18 Security Assessments . . . . .	
Test, Assessment, and Audit Strategies . . . . .	
Designing an Assessment . . . . .	
Validating an Assessment . . . . .	
Testing Technical Controls . . . . .	
Vulnerability Testing . . . . .	
Other Vulnerability Types . . . . .	
Penetration Testing . . . . .	
Red Teaming . . . . .	

813  
813  
814  
815  
817  
817  
819  
822  
827

## ▲Contents

xxiii

Breach Attack Simulations . . . . .	.
Log Reviews . . . . .	.
. . . . .	.
Synthetic Transactions . . . . .	.
. . . . .	.
Code Reviews . . . . .	.
. . . . .	.
Code Testing . . . . .	.
. . . . .	.
Misuse Case Testing . . . . .	.
. . . . .	.
Test Coverage . . . . .	.
. . . . .	.
Interface Testing . . . . .	.
. . . . .	.
Compliance Checks . . . . .	.
. . . . .	.
Conducting Security Audits . . . . .	.
. . . . .	.
Internal Audits . . . . .	.
. . . . .	.
External Audits . . . . .	.
. . . . .	.
Third-Party Audits . . . . .	.
. . . . .	.
Chapter Review . . . . .	.
. . . . .	.
Quick Review . . . . .	.
. . . . .	.
Questions . . . . .	.
. . . . .	.
Answers . . . . .	.
. . . . .	.

828  
828  
832  
833  
834  
835  
837

837  
838  
838  
840  
842  
843  
844  
845  
846  
848

Chapter 19 Measuring Security . . . . .	
Quantifying Security . . . . .	
Security Metrics . . . . .	
Key Performance and Risk Indicators . . . . .	
Security Process Data . . . . .	
Account Management . . . . .	
Backup Verification . . . . .	
Security Training and Security Awareness Training . . . . .	
Disaster Recovery and Business Continuity . . . . .	
Reporting . . . . .	
Analyzing Results . . . . .	
Writing Technical Reports . . . . .	
Executive Summaries . . . . .	
Management Review and Approval . . . . .	
Before the Management Review . . . . .	
Reviewing Inputs . . . . .	
Management Approval . . . . .	
Chapter Review . . . . .	
Quick Review . . . . .	
Questions . . . . .	
Answers . . . . .	

851  
851  
853  
855  
857  
858  
860  
863

867  
869  
870  
872  
873  
875  
876  
876  
877  
877  
878  
879  
881

## Part VII Security Operations

Chapter 20 Managing Security Operations . . . . .	
. . . . .	
Foundational Security Operations Concepts . . . . .	
Accountability . . . . .	
. . . . .	
Need-to-Know/Least Privilege . . . . .	

885  
885  
887  
888

## ▲CISSP All-in-One Exam Guide

xxiv

Separation of Duties and Responsibilities . . . . .	
Privileged Account Management . . . . .	
Job Rotation . . . . .	
. . . . .	
Service Level Agreements . . . . .	
Change Management . . . . .	
. . . . .	
Change Management Practices . . . . .	
Change Management Documentation . . . . .	
Configuration Management . . . . .	
. . . . .	
Baselining . . . . .	
. . . . .	
Provisioning . . . . .	
. . . . .	
Automation . . . . .	
. . . . .	
Resource Protection . . . . .	
. . . . .	
System Images . . . . .	
. . . . .	
Source Files . . . . .	
. . . . .	
Backups . . . . .	

.....	
Vulnerability and Patch Management . . . . .	.
Vulnerability Management . . . . .	.
Patch Management . . . . .	.
Physical Security . . . . .	.
.....	
External Perimeter Security Controls . . . . .	.
Facility Access Control . . . . .	.
.	
Internal Security Controls . . . . .	.
Personnel Access Controls . . . . .	.
Intrusion Detection Systems . . . . .	.
Auditing Physical Access . . . . .	.
Personnel Safety and Security . . . . .	.
.....	
Travel . . . . .	.
.....	
Security Training and Awareness . . . . .	.
Emergency Management . . . . .	.
Duress . . . . .	.
.....	
Chapter Review . . . . .	.
.....	
Quick Review . . . . .	.
..	
Questions . . . . .	.
.....	
Answers . . . . .	.
.....	

888  
889  
889  
890  
891  
891  
893  
893  
894  
894  
895  
895  
896  
896  
896  
900  
900  
903  
906  
906  
916  
924  
924  
925

929  
929  
930  
930  
931  
931  
932  
932  
934  
937

Chapter 21 Security Operations . . . . .	
The Security Operations Center . . . . .	
Elements of a Mature SOC . . . . .	
Threat Intelligence . . . . .	
Preventive and Detective Measures . . . . .	
Firewalls . . . . .	
Intrusion Detection and Prevention Systems . . . . .	
Antimalware Software . . . . .	
Sandboxing . . . . .	
Outsourced Security Services . . . . .	
Honeypots and Honeynets . . . . .	
Artificial Intelligence Tools . . . . .	

939  
939  
940  
941  
944  
945  
967  
969  
972  
973  
974  
976

## ▲Contents

xxv	
Logging and Monitoring . . . . .	
Log Management . . . . .	
Security Information and Event Management . . . . .	
Egress Monitoring . . . . .	
User and Entity Behavior Analytics . . . . .	

Continuous Monitoring . . . . .	
Chapter Review . . . . .	
. . . . .	
Quick Review . . . . .	
. . . . .	
Questions . . . . .	
. . . . .	
Answers . . . . .	
. . . . .	
978	
978	
979	
981	
981	
981	
982	
983	
984	
986	
Chapter 22 Security Incidents . . . . .	
. . . . .	989
Overview of Incident Management . . . . .	
. . . . .	989
Detection . . . . .	
. . . . .	995
Response . . . . .	
. . . . .	996
Mitigation . . . . .	
. . . . .	996
Reporting . . . . .	
. . . . .	997
Recovery . . . . .	
. . . . .	998
Remediation . . . . .	
. . . . .	999
Lessons Learned . . . . .	
. . . . .	999
Incident Response Planning . . . . .	
. . . . .	1000
Roles and Responsibilities . . . . .	
. . . . .	1000
Incident Classification . . . . .	
. . . . .	1002
Notifications . . . . .	
. . . . .	1003
Operational Tasks . . . . .	
. . . . .	1004
Runbooks . . . . .	
. . . . .	1006
Investigations . . . . .	
. . . . .	1006
Motive, Opportunity, and Means . . . . .	1007



Computer Criminal Behavior . . . . .	1008
Evidence Collection and Handling . . . . .	1008
What Is Admissible in Court? . . . . .	1013
Digital Forensics Tools, Tactics, and Procedures . . . . .	1015
Forensic Investigation Techniques . . . . .	1016
Other Investigative Techniques . . . . .	1018
Forensic Artifacts . . . . .	1020
Reporting and Documenting . . . . .	1021
Chapter Review . . . . .	1022
Quick Review . . . . .	1022
Questions . . . . .	1024
Answers . . . . .	1026
Chapter 23 Disasters . . . . .	1029
Recovery Strategies . . . . .	1029
Business Process Recovery . . . . .	1033
Data Backup . . . . .	1034
Documentation . . . . .	1041
Human Resources . . . . .	1042

## ▲CISSP All-in-One Exam Guide

xxvi

Recovery Site Strategies . . . . .	1043
Availability . . . . .	1049
Disaster Recovery Processes . . . . .	1053
Response . . . . .	1055
Personnel . . . . .	1055
Communications . . . . .	1056
Assessment . . . . .	1058
Restoration . . . . .	1058
Training and Awareness . . . . .	1060
Lessons Learned . . . . .	

. . . . .	1061
Testing Disaster Recovery Plans . . . . .	
1061	
Business Continuity . . . . .	
. . . . .	1065
BCP Life Cycle . . . . .	
. . . . .	1065
Information Systems Availability . . . . .	
1067	
End-User Environment . . . . .	
1071	
Chapter Review . . . . .	
. . . . .	1071
Quick Review . . . . .	
. . . . .	1072
Questions . . . . .	
. . . . .	1073
Answers . . . . .	
. . . . .	1075
 Part VIII Software Development Security	
Chapter 24 Software Development . . . . .	
. . . . .	1079
Software Development Life Cycle . . . . .	
. . . . .	1079
Project Management . . . . .	
1081	
Requirements Gathering Phase . . . . .	1082
Design Phase . . . . .	
. . . . .	1083
Development Phase . . . . .	
. . . . .	1087
Testing Phase . . . . .	
. . . . .	1089
Operations and Maintenance Phase . . . . .	1091
Development Methodologies . . . . .	
. . . . .	1095
Waterfall Methodology . . . . .	
1095	
Prototyping . . . . .	
. . . . .	1096
Incremental Methodology . . . . .	
1096	
Spiral Methodology . . . . .	
. . . . .	1098
Rapid Application Development . . . . .	1099
Agile Methodologies . . . . .	
. . . . .	1100
DevOps . . . . .	
. . . . .	1103
DevSecOps . . . . .	
. . . . .	1104
Other Methodologies . . . . .	
1104	

Maturity Models . . . . .	1106
Capability Maturity Model Integration . . . . .	1107
Software Assurance Maturity Model . . . . .	1109

## [Contents](#)

xxvii	
Chapter Review . . . . .	1110
Quick Review . . . . .	1110
Questions . . . . .	1112
Answers . . . . .	1114
Chapter 25 Secure Software . . . . .	1117
Programming Languages and Concepts . . . . .	1118
Assemblers, Compilers, Interpreters . . . . .	1120
Runtime Environments . . . . .	1122
Object-Oriented Programming Concepts . . . . .	1124
Cohesion and Coupling . . . . .	1130
Application Programming Interfaces . . . . .	1132
Software Libraries . . . . .	1132
Secure Software Development . . . . .	1133
Source Code Vulnerabilities . . . . .	1133
Secure Coding Practices . . . . .	1134
Security Controls for Software Development . . . . .	1136
Development Platforms . . . . .	1137
Tool Sets . . . . .	1138
Application Security Testing . . . . .	1139
Continuous Integration and Delivery . . . . .	1140
Security Orchestration, Automation, and Response . . . . .	1141
Software Configuration Management . . . . .	1142
Code Repositories . . . . .	1143
Software Security Assessments . . . . .	1144
Risk Analysis and Mitigation . . . . .	1144
Change Management . . . . .	1145

Assessing the Security of Acquired Software . . . . .	1145
Commercial Software . . . . .	1146
Open-Source Software . . . . .	1146
Third-Party Software . . . . .	1147
Managed Services . . . . .	1148
Chapter Review . . . . .	1148
Quick Review . . . . .	1148
Questions . . . . .	1150
Answers . . . . .	1152
Appendix A Comprehensive Questions . . . . .	1155
Answers . . . . .	1189
Appendix B Objective Map	

. . . . .	1209
Appendix C About the Online Content . . . . .	1225
System Requirements . . . . .	1225
Your Total Seminars Training Hub Account . . . . .	1225
Privacy Notice . . . . .	1225

## ▲CISSP All-in-One Exam Guide

xxviii	
Single User License Terms and Conditions . . . . .	1225
TotalTester Online . . . . .	1227
Graphical Questions . . . . .	1227
Online Flash Cards . . . . .	1228
Single User License Terms and Conditions . . . . .	1228
Technical Support . . . . .	1229
Glossary	
Index	

. . . . .	
-----------	--

. . . . . 1231

. . . . .  
. . . . . 1253

#### ▲FROM THE AUTHOR

Thank you for investing your resources in this ninth edition of the CISSP All-in-One

Exam Guide. I am confident you'll find it helpful, not only as you prepare for the CISSP

exam, but as a reference in your future professional endeavors. That was one of the overarching goals of Shon Harris when she wrote the first six editions and is something I've

strived to uphold in the last three. It is not always easy, but I think you'll be pleased with

how we've balanced these two requirements.

(ISC)2 does a really good job of grounding the CISSP Common Body of Knowledge (CBK) in real-world applications, but (let's face it) there's always a lot of room for

discussion and disagreements. There are very few topics in cybersecurity (or pretty much

any other field) on which there is universal agreement. To balance the content of this

book between exam preparation and the murkiness of real-world applications, we've

included plenty of comments and examples drawn from our experiences.

I say "our experiences" deliberately because the voice of Shon remains vibrant, informative, and entertaining in this edition, years after her passing. I've preserved as many of

her insights as possible while ensuring the content is up to date and relevant. I also strove

to maintain the conversational tone that was such a hallmark of her work. The result is

a book that (I hope) reads more like an essay (or even a story) than a textbook but is

grounded in good pedagogy. It should be easy to read but still prepare you for the exam.

Speaking of the exam, the changes that (ISC)2 made to the CBK in 2021 are not dramatic but are still significant. Each domain was tweaked in some way, and seven of

the eight domains had multiple topics added (domain 1 was the exception here). These

changes, coupled with the number of topics that were growing stale in the eighth edition

of this book, prompted me to completely restructure this edition. I tore each domain and

topic down to atomic particles and then re-engineered the entire book to integrate the

new objectives, which are listed in Table 1.

Domain 2: Asset Security

2.4

Manage data lifecycle

#### 2.4.1

Data roles (i.e., owners, controllers, custodians, processors, users/subjects)

#### 2.4.3

Data location

#### 2.4.4

Data maintenance

#### 2.5

Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

Domain 3: Security Architecture and Engineering  
(Under 3.7 Understand methods of cryptanalytic attacks)

#### 3.7.1

Brute force

#### 3.7.4

Frequency analysis

Table 1 CBK 2021: New Objectives (continued)

xxix

▲CISSP All-in-One Exam Guide

xxx

Domain 3: Security Architecture and Engineering

#### 3.7.6

Implementation attacks

#### 3.7.8

Fault injection

#### 3.7.9

Timing

#### 3.7.10

Man-in-the-Middle (MITM)

#### 3.7.11

Pass the hash

3.7.12

Kerberos exploitation

3.7.13

Ransomware

(Under 3.9 Design site and facility security controls)

3.9.9

Power (e.g., redundant, backup)

Domain 4: Communication and Network Security

(Under 4.1 Assess and implement secure design principles in network architectures)

4.1.3

Secure protocols

4.1.6

Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local

Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))

4.1.8

Cellular networks (e.g., 4G, 5G)

(Under 4.3 Implement secure communication channels according to design)

4.3.6

Third-party connectivity

Domain 5: Identity and Access Management (IAM)

(Under 5.1 Control physical and logical access to assets)

5.1.5

Applications

(Under 5.2 Manage identification and authentication of people, devices, and services)

5.2.8

Single Sign On (SSO)

5.2.9

Just-In-Time (JIT)

(Under 5.4 Implement and manage authorization mechanisms)

#### 5.4.6

Risk based access control

(Under 5.5 Manage the identity and access provisioning lifecycle)

#### 5.5.3

Role definition (e.g., people assigned to new roles)

#### 5.5.4

Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)

#### 5.6

Implement authentication systems

#### 5.6.1

OpenID Connect (OIDC)/Open Authorization (OAuth)

#### 5.6.2

Security Assertion Markup Language (SAML)

#### 5.6.3

Kerberos

#### 5.6.4

Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

Domain 6: Security Assessment and Testing  
(Under 6.2 Conduct security control testing)

#### 6.2.9

Breach attack simulations

#### 6.2.10

Compliance checks

Table 1 CBK 2021: New Objectives

▲From the Author

xxxi

Domain 6: Security Assessment and Testing  
(Under 6.3 Collect security process data (e.g., technical and administrative))

#### 6.3.6



Disaster Recovery (DR) and Business Continuity (BC)

(Under 6.4 Analyze test output and generate report)

6.4.1

Remediation

6.4.2

Exception handling

6.4.3

Ethical disclosure

Domain 7: Security Operations

(Under 7.1 Understand and comply with investigations)

7.1.5

Artifacts (e.g., computer, network, mobile device)

(Under 7.2 Conduct logging and monitoring activities)

7.2.5

Log management

7.2.6

Threat intelligence (e.g., threat feeds, threat hunting)

7.2.7

User and Entity Behavior Analytics (UEBA)

(Under 7.7 Operate and maintain detective and preventative measures)

7.7.8

Machine learning and Artificial Intelligence (AI) based tools

(Under 7.11 Implement Disaster Recovery (DR) processes)

7.11.7

Lessons learned

Domain 8: Software Development Security

(Under 8.2 Identify and apply security controls in software development ecosystems)

8.2.1

Programming languages

8.2.2

Libraries

8.2.3

Tool sets

8.2.5

Runtime

8.2.6

Continuous Integration and Continuous Delivery (CI/CD)

8.2.7

Security Orchestration, Automation, and Response (SOAR)

8.2.10

Application security testing (e.g., Static Application Security Testing (SAST),  
Dynamic  
Application Security Testing (DAST))

(Under 8.4 Assess security impact of acquired software)

8.4.1

Commercial-off-the-shelf (COTS)

8.4.2

Open source

8.4.3

Third-party

8.4.4

Managed services (e.g., Software as a Service (SaaS), Infrastructure as a  
Service (IaaS),  
Platform as a Service (PaaS))

(Under 8.5 Define and apply secure coding guidelines and standards)

8.5.4

Software-defined security

Table 1 CBK 2021: New Objectives (continued)

▲CISSP All-in-One Exam Guide

xxxii

Note that some of these objectives were implicit in the previous (2018) version  
of