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

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

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

This page intentionally left blank

↟CONTENTS AT A GLANCE

↟Contents

↟Contents

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)

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

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)

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