

*“All-in-One Is All You Need.”*

ALL-IN-ONE

# CISSP®

EXAM GUIDE  
NINTH EDITION

*Fully updated coverage  
of all 8 domains for the  
2021 Certified Information  
Systems Security  
Professional exam*

*Ideal as both a study guide  
and an on-the-job reference*

*Filled with practice exam  
questions and in-depth  
explanations*

**Mc  
Graw  
Hill**

**Online content  
includes:**

- 1400+ practice exam questions
- Graphical question quizzes
- Test engine that provides full-length practice exams and customizable quizzes by chapter or exam domain
- Access to Flash cards

FERNANDO MAYMÍ, PhD, CISSP  
SHON HARRIS, CISSP

## 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 GISE,  
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

<b>Part I</b>	Security and Risk Management	
<b>Chapter 1</b>	Cybersecurity Governance .....	3
<b>Chapter 2</b>	Risk Management .....	53
<b>Chapter 3</b>	Compliance .....	125
<b>Chapter 4</b>	Frameworks .....	171
<b>Part II</b>	Asset Security	
<b>Chapter 5</b>	Assets .....	213
<b>Chapter 6</b>	Data Security .....	253
<b>Part III</b>	Security Architecture and Engineering	
<b>Chapter 7</b>	System Architectures .....	283
<b>Chapter 8</b>	Cryptology .....	317
<b>Chapter 9</b>	Security Architectures .....	385
<b>Chapter 10</b>	Site and Facility Security .....	417
<b>Part IV</b>	Communication and Network Security	
<b>Chapter 11</b>	Networking Fundamentals .....	469
<b>Chapter 12</b>	Wireless Networking .....	559
<b>Chapter 13</b>	Securing the Network .....	597
<b>Chapter 14</b>	Network Components .....	643
<b>Chapter 15</b>	Secure Communications Channels .....	681
<b>Part V</b>	Identity and Access Management	
<b>Chapter 16</b>	Identity and Access Fundamentals .....	715
<b>Chapter 17</b>	Managing Identities and Access .....	765

<b>Part VI</b>	Security Assessment and Testing	
<b>Chapter 18</b>	Security Assessments .....	813
<b>Chapter 19</b>	Measuring Security.....	851
<b>Part VII</b>	Security Operations	
<b>Chapter 20</b>	Managing Security Operations.....	885
<b>Chapter 21</b>	Security Operations .....	939
<b>Chapter 22</b>	Security Incidents .....	989
<b>Chapter 23</b>	Disasters.....	1029
<b>Part VIII</b>	Software Development Security	
<b>Chapter 24</b>	Software Development .....	1079
<b>Chapter 25</b>	Secure Software .....	1117
<b>Appendix A</b>	Comprehensive Questions .....	1155
<b>Appendix B</b>	Objective Map .....	1209
<b>Appendix C</b>	About the Online Content.....	1225
	Glossary .....	1231
	Index.....	1253

---

# CONTENTS

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

## **Part I** Security and Risk Management

<b>Chapter 1</b>	Cybersecurity Governance .....	3
	Fundamental Cybersecurity Concepts and Terms .....	4
	Confidentiality .....	5
	Integrity .....	5
	Availability .....	6
	Authenticity .....	6
	Nonrepudiation .....	6
	Balanced Security .....	7
	Other Security Terms .....	8
	Security Governance Principles .....	10
	Aligning Security to Business Strategy .....	13
	Organizational Processes .....	17
	Organizational Roles and Responsibilities .....	18
	Security Policies, Standards, Procedures, and Guidelines .....	25
	Security Policy .....	27
	Standards .....	29
	Baselines .....	31
	Guidelines .....	32
	Procedures .....	32
	Implementation .....	32
	Personnel Security .....	33
	Candidate Screening and Hiring .....	35
	Employment Agreements and Policies .....	36
	Onboarding, Transfers, and Termination Processes .....	37
	Vendors, Consultants, and Contractors .....	39
	Compliance Policies .....	39
	Privacy Policies .....	40
	Security Awareness, Education, and Training Programs .....	40
	Degree or Certification? .....	40
	Methods and Techniques to Present	
	Awareness and Training .....	41

Periodic Content Reviews	43
Program Effectiveness Evaluation	43
Professional Ethics	44
(ISC) <sup>2</sup> Code of Professional Ethics	44
Organizational Code of Ethics	45
The Computer Ethics Institute	45
Chapter Review	46
Quick Review	46
Questions	48
Answers	51
<b>Chapter 2 Risk Management</b>	<b>53</b>
Risk Management Concepts	53
Holistic Risk Management	54
Information Systems Risk Management Policy	56
The Risk Management Team	56
The Risk Management Process	57
Overview of Vulnerabilities and Threats	58
Identifying Threats and Vulnerabilities	62
Assessing Risks	63
Asset Valuation	65
Risk Assessment Teams	66
Methodologies for Risk Assessment	67
Risk Analysis Approaches	72
Qualitative Risk Analysis	76
Responding to Risks	79
Total Risk vs. Residual Risk	81
Countermeasure Selection and Implementation	81
Types of Controls	83
Control Assessments	88
Monitoring Risks	91
Effectiveness Monitoring	91
Change Monitoring	92
Compliance Monitoring	93
Risk Reporting	94
Continuous Improvement	95
Supply Chain Risk Management	96
Upstream and Downstream Suppliers	98
Risks Associated with Hardware, Software, and Services	98
Other Third-Party Risks	99
Minimum Security Requirements	100
Service Level Agreements	101
Business Continuity	101
Standards and Best Practices	104
Making BCM Part of the Enterprise Security Program	106
Business Impact Analysis	108

Chapter Review	116
Quick Review	116
Questions	118
Answers	121
<b>Chapter 3</b> Compliance	125
Laws and Regulations	125
Types of Legal Systems	126
Common Law Revisited	129
Cybercrimes and Data Breaches	130
Complexities in Cybercrime	132
The Evolution of Attacks	134
International Issues	138
Data Breaches	139
Import/Export Controls	145
Transborder Data Flow	146
Privacy	147
Licensing and Intellectual Property Requirements	147
Trade Secret	148
Copyright	149
Trademark	150
Patent	151
Internal Protection of Intellectual Property	152
Software Piracy	153
Compliance Requirements	155
Contractual, Legal, Industry Standards, and Regulatory Requirements	156
Privacy Requirements	158
Liability and Its Ramifications	158
Requirements for Investigations	161
Administrative	161
Criminal	162
Civil	162
Regulatory	162
Chapter Review	162
Quick Review	163
Questions	165
Answers	168
<b>Chapter 4</b> Frameworks	171
Overview of Frameworks	171
Risk Frameworks	173
NIST RMF	173
ISO/IEC 27005	177
OCTAVE	178
FAIR	179

Information Security Frameworks .....	179
Security Program Frameworks .....	180
Security Control Frameworks .....	183
Enterprise Architecture Frameworks .....	189
Why Do We Need Enterprise Architecture Frameworks? ....	191
Zachman Framework .....	192
The Open Group Architecture Framework .....	194
Military-Oriented Architecture Frameworks .....	195
Other Frameworks .....	196
ITIL .....	196
Six Sigma .....	197
Capability Maturity Model .....	197
Putting It All Together .....	199
Chapter Review .....	203
Quick Review .....	203
Questions .....	205
Answers .....	208

## **Part II** Asset Security

<b>Chapter 5</b> Assets .....	213
Information and Assets .....	214
Identification .....	214
Classification .....	215
Physical Security Considerations .....	220
Protecting Mobile Devices .....	220
Paper Records .....	221
Safes .....	221
Managing the Life Cycle of Assets .....	222
Ownership .....	223
Inventories .....	224
Secure Provisioning .....	227
Asset Retention .....	228
Data Life Cycle .....	230
Data Acquisition .....	230
Data Storage .....	232
Data Use .....	237
Data Sharing .....	238
Data Archival .....	239
Data Destruction .....	240
Data Roles .....	244
Chapter Review .....	245
Quick Review .....	245
Questions .....	247
Answers .....	250

<b>Chapter 6</b>	<b>Data Security</b>	253
	Data Security Controls	253
	Data States	254
	Standards	258
	Scoping and Tailoring	258
	Data Protection Methods	258
	Digital Asset Management	261
	Digital Rights Management	263
	Data Loss Prevention	265
	Cloud Access Security Broker	275
	Chapter Review	276
	Quick Review	276
	Questions	277
	Answers	279

### **Part III** Security Architecture and Engineering

<b>Chapter 7</b>	<b>System Architectures</b>	283
	General System Architectures	283
	Client-Based Systems	284
	Server-Based Systems	284
	Database Systems	285
	High-Performance Computing Systems	288
	Industrial Control Systems	289
	Devices	291
	Distributed Control System	293
	Supervisory Control and Data Acquisition	294
	ICS Security	294
	Virtualized Systems	296
	Virtual Machines	296
	Containerization	298
	Microservices	299
	Serverless	299
	Cloud-Based Systems	301
	Software as a Service	302
	Platform as a Service	303
	Infrastructure as a Service	304
	Everything as a Service	304
	Cloud Deployment Models	305
	Pervasive Systems	305
	Embedded Systems	306
	Internet of Things	306
	Distributed Systems	307
	Edge Computing Systems	308



	Chapter Review .....	310
	Quick Review .....	310
	Questions .....	311
	Answers .....	314
<b>Chapter 8</b>	<b>Cryptology .....</b>	<b>317</b>
	The History of Cryptography .....	317
	Cryptography Definitions and Concepts .....	321
	Cryptosystems .....	323
	Kerckhoffs' Principle .....	324
	The Strength of the Cryptosystem .....	325
	One-Time Pad .....	325
	Cryptographic Life Cycle .....	328
	Cryptographic Methods .....	328
	Symmetric Key Cryptography .....	329
	Asymmetric Key Cryptography .....	335
	Elliptic Curve Cryptography .....	342
	Quantum Cryptography .....	344
	Hybrid Encryption Methods .....	346
	Integrity .....	351
	Hashing Functions .....	351
	Message Integrity Verification .....	354
	Public Key Infrastructure .....	359
	Digital Certificates .....	359
	Certificate Authorities .....	360
	Registration Authorities .....	362
	PKI Steps .....	362
	Key Management .....	364
	Attacks Against Cryptography .....	367
	Key and Algorithm Attacks .....	367
	Implementation Attacks .....	370
	Other Attacks .....	372
	Chapter Review .....	375
	Quick Review .....	376
	Questions .....	379
	Answers .....	381
<b>Chapter 9</b>	<b>Security Architectures .....</b>	<b>385</b>
	Threat Modeling .....	385
	Attack Trees .....	386
	STRIDE .....	387
	The Lockheed Martin Cyber Kill Chain .....	387
	The MITRE ATT&CK Framework .....	389
	Why Bother with Threat Modeling .....	389

Secure Design Principles	390
Defense in Depth	390
Zero Trust	392
Trust But Verify	392
Shared Responsibility	392
Separation of Duties	393
Least Privilege	394
Keep It Simple	395
Secure Defaults	396
Fail Securely	396
Privacy by Design	397
Security Models	397
Bell-LaPadula Model	398
Biba Model	399
Clark-Wilson Model	400
Noninterference Model	400
Brewer and Nash Model	402
Graham-Denning Model	402
Harrison-Ruzzo-Ullman Model	402
Security Requirements	404
Security Capabilities of Information Systems	404
Trusted Platform Module	404
Hardware Security Module	406
Self-Encrypting Drive	407
Bus Encryption	407
Secure Processing	408
Chapter Review	411
Quick Review	412
Questions	413
Answers	415
<b>Chapter 10 Site and Facility Security</b>	<b>417</b>
Site and Facility Design	417
Security Principles	418
The Site Planning Process	423
Crime Prevention Through Environmental Design	427
Designing a Physical Security Program	433
Site and Facility Controls	441
Work Area Security	441
Data Processing Facilities	443
Distribution Facilities	446
Storage Facilities	447
Utilities	448
Fire Safety	454
Environmental Issues	461

Chapter Review .....	461
Quick Review .....	461
Questions .....	463
Answers .....	465

## **Part IV** Communication and Network Security

<b>Chapter 11</b>	<b>Networking Fundamentals .....</b>	<b>469</b>
	Data Communications Foundations .....	469
	Network Reference Models .....	470
	Protocols .....	471
	Application Layer .....	474
	Presentation Layer .....	475
	Session Layer .....	477
	Transport Layer .....	479
	Network Layer .....	480
	Data Link Layer .....	480
	Physical Layer .....	483
	Functions and Protocols in the OSI Model .....	483
	Tying the Layers Together .....	485
	Local Area Networks .....	487
	Network Topology .....	487
	Medium Access Control Mechanisms .....	489
	Layer 2 Protocols .....	494
	Transmission Methods .....	499
	Layer 2 Security Standards .....	500
	Internet Protocol Networking .....	502
	TCP .....	503
	IP Addressing .....	510
	IPv6 .....	512
	Address Resolution Protocol .....	515
	Dynamic Host Configuration Protocol .....	517
	Internet Control Message Protocol .....	520
	Simple Network Management Protocol .....	522
	Domain Name Service .....	524
	Network Address Translation .....	531
	Routing Protocols .....	533
	Intranets and Extranets .....	537
	Metropolitan Area Networks .....	538
	Metro Ethernet .....	539
	Wide Area Networks .....	540
	Dedicated Links .....	541
	WAN Technologies .....	543

Chapter Review	552
Quick Review	553
Questions	555
Answers	557
<b>Chapter 12 Wireless Networking</b>	<b>559</b>
Wireless Communications Techniques	559
Spread Spectrum	561
Orthogonal Frequency Division Multiplexing	563
Wireless Networking Fundamentals	564
WLAN Components	564
WLAN Standards	565
Other Wireless Network Standards	568
Other Important Standards	573
Evolution of WLAN Security	574
802.11	575
802.11i	576
802.11w	578
WPA3	578
802.1X	579
Best Practices for Securing WLANs	582
Mobile Wireless Communication	582
Multiple Access Technologies	584
Generations of Mobile Wireless	585
Satellites	588
Chapter Review	590
Quick Review	590
Questions	592
Answers	594
<b>Chapter 13 Securing the Network</b>	<b>597</b>
Applying Secure Design Principles to Network Architectures	597
Secure Networking	599
Link Encryption vs. End-to-End Encryption	600
TLS	602
VPN	605
Secure Protocols	611
Web Services	611
Domain Name System	616
Electronic Mail	621
Multilayer Protocols	626
Distributed Network Protocol 3	626
Controller Area Network Bus	627
Modbus	627

Converged Protocols	627
Encapsulation	628
Fiber Channel over Ethernet	628
Internet Small Computer Systems Interface	629
Network Segmentation	629
VLANs	630
Virtual eXtensible Local Area Network	632
Software-Defined Networks	632
Software-Defined Wide Area Network	635
Chapter Review	635
Quick Review	636
Questions	638
Answers	640
<b>Chapter 14 Network Components</b>	<b>643</b>
Transmission Media	643
Types of Transmission	644
Cabling	648
Bandwidth and Throughput	654
Network Devices	655
Repeaters	655
Bridges	656
Switches	657
Routers	660
Gateways	662
Proxy Servers	663
PBXs	665
Network Access Control Devices	667
Network Diagramming	668
Operation of Hardware	670
Endpoint Security	673
Content Distribution Networks	674
Chapter Review	674
Quick Review	675
Questions	677
Answers	678
<b>Chapter 15 Secure Communications Channels</b>	<b>681</b>
Voice Communications	682
Public Switched Telephone Network	682
DSL	683
ISDN	685
Cable Modems	686
IP Telephony	687

Multimedia Collaboration .....	693
Meeting Applications .....	694
Unified Communications .....	695
Remote Access .....	696
VPN .....	697
Desktop Virtualization .....	699
Secure Shell .....	701
Data Communications .....	702
Network Sockets .....	703
Remote Procedure Calls .....	703
Virtualized Networks .....	704
Third-Party Connectivity .....	705
Chapter Review .....	707
Quick Review .....	707
Questions .....	709
Answers .....	711

## **Part V** Identity and Access Management

<b>Chapter 16</b> Identity and Access Fundamentals .....	715
Identification, Authentication, Authorization, and Accountability ....	715
Identification and Authentication .....	718
Knowledge-Based Authentication .....	720
Biometric Authentication .....	723
Ownership-Based Authentication .....	729
Credential Management .....	736
Password Managers .....	736
Password Synchronization .....	737
Self-Service Password Reset .....	737
Assisted Password Reset .....	738
Just-in-Time Access .....	738
Registration and Proofing of Identity .....	738
Profile Update .....	740
Session Management .....	740
Accountability .....	741
Identity Management .....	745
Directory Services .....	747
Directories' Role in Identity Management .....	748
Single Sign-On .....	750
Federated Identity Management .....	752
Federated Identity with a Third-Party Service .....	754
Integration Issues .....	754
On-Premise .....	755
Cloud .....	756
Hybrid .....	756

Chapter Review	756
Quick Review	757
Questions	759
Answers	762
<b>Chapter 17 Managing Identities and Access</b>	<b>765</b>
Authorization Mechanisms	765
Discretionary Access Control	766
Mandatory Access Control	768
Role-Based Access Control	771
Rule-Based Access Control	774
Attribute-Based Access Control	774
Risk-Based Access Control	775
Implementing Authentication and Authorization Systems	776
Access Control and Markup Languages	776
OAuth	782
OpenID Connect	783
Kerberos	784
Remote Access Control Technologies	789
Managing the Identity and Access Provisioning Life Cycle	795
Provisioning	796
Access Control	796
Compliance	796
Configuration Management	799
Deprovisioning	800
Controlling Physical and Logical Access	801
Information Access Control	801
System and Application Access Control	802
Access Control to Devices	802
Facilities Access Control	802
Chapter Review	804
Quick Review	804
Questions	805
Answers	808

## **Part VI Security Assessment and Testing**

<b>Chapter 18 Security Assessments</b>	<b>813</b>
Test, Assessment, and Audit Strategies	813
Designing an Assessment	814
Validating an Assessment	815
Testing Technical Controls	817
Vulnerability Testing	817
Other Vulnerability Types	819
Penetration Testing	822
Red Teaming	827

Breach Attack Simulations	828
Log Reviews	828
Synthetic Transactions	832
Code Reviews	833
Code Testing	834
Misuse Case Testing	835
Test Coverage	837
Interface Testing	837
Compliance Checks	838
Conducting Security Audits	838
Internal Audits	840
External Audits	842
Third-Party Audits	843
Chapter Review	844
Quick Review	845
Questions	846
Answers	848
<b>Chapter 19 Measuring Security</b>	<b>851</b>
Quantifying Security	851
Security Metrics	853
Key Performance and Risk Indicators	855
Security Process Data	857
Account Management	858
Backup Verification	860
Security Training and Security Awareness Training	863
Disaster Recovery and Business Continuity	867
Reporting	869
Analyzing Results	870
Writing Technical Reports	872
Executive Summaries	873
Management Review and Approval	875
Before the Management Review	876
Reviewing Inputs	876
Management Approval	877
Chapter Review	877
Quick Review	878
Questions	879
Answers	881
<b>Part VII Security Operations</b>	
<b>Chapter 20 Managing Security Operations</b>	<b>885</b>
Foundational Security Operations Concepts	885
Accountability	887
Need-to-Know/Least Privilege	888



Separation of Duties and Responsibilities .....	888
Privileged Account Management .....	889
Job Rotation .....	889
Service Level Agreements .....	890
Change Management .....	891
Change Management Practices .....	891
Change Management Documentation .....	893
Configuration Management .....	893
Baselining .....	894
Provisioning .....	894
Automation .....	895
Resource Protection .....	895
System Images .....	896
Source Files .....	896
Backups .....	896
Vulnerability and Patch Management .....	900
Vulnerability Management .....	900
Patch Management .....	903
Physical Security .....	906
External Perimeter Security Controls .....	906
Facility Access Control .....	916
Internal Security Controls .....	924
Personnel Access Controls .....	924
Intrusion Detection Systems .....	925
Auditing Physical Access .....	929
Personnel Safety and Security .....	929
Travel .....	930
Security Training and Awareness .....	930
Emergency Management .....	931
Duress .....	931
Chapter Review .....	932
Quick Review .....	932
Questions .....	934
Answers .....	937
<b>Chapter 21 Security Operations .....</b>	<b>939</b>
The Security Operations Center .....	939
Elements of a Mature SOC .....	940
Threat Intelligence .....	941
Preventive and Detective Measures .....	944
Firewalls .....	945
Intrusion Detection and Prevention Systems .....	967
Antimalware Software .....	969
Sandboxing .....	972
Outsourced Security Services .....	973
Honeypots and Honeynets .....	974
Artificial Intelligence Tools .....	976

Logging and Monitoring .....	978
Log Management .....	978
Security Information and Event Management .....	979
Egress Monitoring .....	981
User and Entity Behavior Analytics .....	981
Continuous Monitoring .....	981
Chapter Review .....	982
Quick Review .....	983
Questions .....	984
Answers .....	986
<b>Chapter 22 Security Incidents .....</b>	<b>989</b>
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
<b>Chapter 23 Disasters .....</b>	<b>1029</b>
Recovery Strategies .....	1029
Business Process Recovery .....	1033
Data Backup .....	1034
Documentation .....	1041
Human Resources .....	1042

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

<b>Chapter 24</b> 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

Chapter Review	1110
Quick Review	1110
Questions	1112
Answers	1114
<b>Chapter 25 Secure Software</b>	<b>1117</b>
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
<b>Appendix A Comprehensive Questions</b>	<b>1155</b>
Answers	1189
<b>Appendix B Objective Map</b>	<b>1209</b>
<b>Appendix C About the Online Content</b>	<b>1225</b>
System Requirements	1225
Your Total Seminars Training Hub Account	1225
Privacy Notice	1225

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 .....	1231
Index .....	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)<sup>2</sup> 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)<sup>2</sup> 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*)

### 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

**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 the CBK and were therefore covered in the eighth edition of this book. The fact that they are now explicit is an indication of their increased importance both in the exam and in the real world. (Please pay particular attention to these as you prepare for the exam.) All in all, this ninth edition is significantly different (and improved) when compared to the previous one. I think you'll agree. Thank you, again, for investing in this ninth edition.

---

# ACKNOWLEDGMENTS

I would like to thank all the people who work in the information security industry who are driven by their passion, dedication, and a true sense of doing right. These selfless professionals sacrifice their personal time to prevent, block, and respond to the relentless efforts of malicious actors around the world. We all sleep more peacefully at night because you remain at the ready.

In this ninth edition, I would also like to thank the following:

- Ronald C. Dodge, Jr., who introduced me to Shon Harris and, in so doing, started me off on one of the best adventures of my life
- Kathy Conlon, who, more than anyone else, set the conditions that led to nine editions of this book
- Carol Remicci
- David Harris
- The men and women of our armed forces, who selflessly defend our way of life

*This page intentionally left blank*

---

## WHY BECOME A CISSP?

As our world changes, the need for improvements in security and technology continues to grow. Organizations around the globe are desperate to identify and recruit talented and experienced security professionals to help protect their assets and remain competitive. As a Certified Information Systems Security Professional (CISSP), you will be seen as a security professional of proven ability who has successfully met a predefined standard of knowledge and experience that is well understood and respected throughout the industry. By keeping this certification current, you will demonstrate your dedication to staying abreast of security developments.

Consider some of the reasons for attaining a CISSP certification:

- To broaden your current knowledge of security concepts and practices
- To demonstrate your expertise as a seasoned security professional
- To become more marketable in a competitive workforce
- To increase your salary and be eligible for more employment opportunities
- To bring improved security expertise to your current occupation
- To show a dedication to the security discipline

The CISSP certification helps organizations identify which individuals have the ability, knowledge, and experience necessary to implement solid security practices; perform risk analysis; identify necessary countermeasures; and help the organization as a whole protect its facility, network, systems, and information. The CISSP certification also shows potential employers you have achieved a level of proficiency and expertise in skill sets and knowledge required by the security industry. The increasing importance placed on security by organizations of all sizes will only continue in the future, leading to even greater demands for highly skilled security professionals. The CISSP certification shows that a respected third-party organization has recognized an individual's technical and theoretical knowledge and expertise, and distinguishes that individual from those who lack this level of knowledge.

Understanding and implementing security practices is an essential part of being a good network administrator, programmer, or engineer. Job descriptions that do not specifically target security professionals still often require that a potential candidate have a good understanding of security concepts and how to implement them. Due to staff size and budget restraints, many organizations can't afford separate network and security staffs. But they still believe security is vital to their organization. Thus, they often try to combine knowledge of technology and security into a single role. With a CISSP designation, you can put yourself head and shoulders above other individuals in this regard.

## The CISSP Exam

Because the CISSP exam covers the eight domains making up the CISSP CBK, it is often described as being “an inch deep and a mile wide,” a reference to the fact that many questions on the exam are not very detailed and do not require you to be an expert in every subject. However, the questions do require you to be familiar with many *different* security subjects.

The CISSP exam comes in two versions depending on the language in which the test is written. The English version uses Computerized Adaptive Testing (CAT) in which the number of questions you are asked depends on your measured level of knowledge but ranges from 100 to 150. Of these, 25 questions will not count toward your score, as they are being evaluated for inclusion in future exams (this is why they are sometimes called pre-test questions). Essentially, the easier it is for the test software to determine your level of proficiency, the fewer questions you’ll get. Regardless of how many questions you are presented, though, you will have no more than three hours to complete the test. When the system has successfully assessed your level of knowledge, the test will end regardless of how long you’ve been at it.



**EXAM TIP** CAT questions are intentionally designed to “feel” hard (based on the system’s estimate of your knowledge), so don’t be discouraged. Just don’t get bogged down because you must answer at least 100 questions in three hours.

The non-English version of the CISSP exam is also computer-based but is linear, fixed-form (not adaptive) and comprises 250 questions, which must be answered in no more than six hours. Like the CAT version, 25 questions are pre-test (unscored), so you will be graded on the other 225 questions. The 25 research questions are integrated into the exam, so you won’t know which go toward your final grade.

Regardless of which version of the exam you take, you need a score of 700 points out of a possible 1,000. In both versions, you can expect multiple choice and innovative questions. Innovative questions incorporate drag-and-drop (i.e., take a term or item and drag it to the correct position in the frame) or hotspot (i.e., click the item or term that correctly answers the question) interfaces, but are otherwise weighed and scored just like any other question. The questions are pulled from a much larger question bank to ensure the exam is as unique as possible for each examinee. In addition, the test bank constantly changes and evolves to more accurately reflect the real world of security. The exam questions are continually rotated and replaced in the bank as necessary. Questions are weighted based on their difficulty; not all questions are worth the same number of points. The exam is not product or vendor oriented, meaning no questions will be specific to certain products or vendors (for instance, Windows, Unix, or Cisco). Instead, you will be tested on the security models and methodologies used by these types of systems.



**EXAM TIP** There is no penalty for guessing. If you can’t come up with the right answer in a reasonable amount of time, then you should guess and move on to the next question.

(ISC)<sup>2</sup>, which stands for International Information Systems Security Certification Consortium, also includes scenario-based questions in the CISSP exam. These questions

present a short scenario to the test taker rather than asking the test taker to identify terms and/or concepts. The goal of the scenario-based questions is to ensure that test takers not only know and understand the concepts within the CBK but also can apply this knowledge to real-life situations. This is more practical because in the real world you won't be challenged by having someone asking you, "What is the definition of collusion?" You need to know how to detect and prevent collusion from taking place, in addition to knowing the definition of the term.

After passing the exam, you will be asked to supply documentation, supported by a sponsor, proving that you indeed have the type of experience required to obtain CISSP certification. The sponsor must sign a document vouching for the security experience you are submitting. So, make sure you have this sponsor lined up prior to registering for the exam and providing payment. You don't want to pay for and pass the exam, only to find you can't find a sponsor for the final step needed to achieve your certification.

The reason behind the sponsorship requirement is to ensure that those who achieve the certification have real-world experience to offer organizations. Book knowledge is extremely important for understanding theory, concepts, standards, and regulations, but it can never replace hands-on experience. Proving your practical experience supports the relevance of the certification.

A small sample group of individuals selected at random will be audited after passing the exam. The audit consists mainly of individuals from (ISC)<sup>2</sup> calling on the candidates' sponsors and contacts to verify the test taker's related experience.

One of the factors that makes the CISSP exam challenging is that most candidates, although they work in the security field, are not necessarily familiar with all eight CBK domains. If a security professional is considered an expert in vulnerability testing or application security, for example, she may not be familiar with physical security, cryptography, or forensics. Thus, studying for this exam will broaden your knowledge of the security field.

The exam questions address the eight CBK security domains, which are described in Table 2.

Domain	Description
Security and Risk Management	<p>This domain covers many of the foundational concepts of information systems security. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• Professional ethics</li> <li>• Security governance and compliance</li> <li>• Legal and regulatory issues</li> <li>• Personnel security policies</li> <li>• Risk management</li> </ul>
Asset Security	<p>This domain examines the protection of assets throughout their life cycle. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• Identifying and classifying information and assets</li> <li>• Establishing information and asset handling requirements</li> <li>• Provisioning resources securely</li> <li>• Managing the data life cycle</li> <li>• Determining data security controls and compliance requirements</li> </ul>

**Table 2** Security Domains that Make up the CISSP CBK (*continued*)

Domain	Description
Security Architecture and Engineering	<p>This domain examines the development of information systems that remain secure in the face of a myriad of threats. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• Secure design principles</li> <li>• Security models</li> <li>• Selection of effective controls</li> <li>• Cryptography</li> <li>• Physical security</li> </ul>
Communication and Network Security	<p>This domain examines network architectures, communications technologies, and network protocols with the goal of understanding how to secure them. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• Secure network architectures</li> <li>• Secure network components</li> <li>• Secure communications channels</li> </ul>
Identity and Access Management (IAM)	<p>Identity and access management is one of the most important topics in information security. This domain covers the interactions between users and systems as well as between systems and other systems. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• Controlling physical and logical access to assets</li> <li>• Identification and authentication</li> <li>• Authorization mechanisms</li> <li>• Identity and access provisioning life cycle</li> <li>• Implementing authentication systems</li> </ul>
Security Assessment and Testing	<p>This domain examines ways to verify the security of our information systems. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• Assessment and testing strategies</li> <li>• Testing security controls</li> <li>• Collecting security process data</li> <li>• Analyzing and reporting results</li> <li>• Conducting and facilitating audits</li> </ul>
Security Operations	<p>This domain covers the many activities involved in the daily business of maintaining the security of our networks. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• Investigations</li> <li>• Logging and monitoring</li> <li>• Change and configuration management</li> <li>• Incident management</li> <li>• Disaster recovery</li> </ul>
Software Development Security	<p>This domain examines the application of security principles to the acquisition and development of software systems. Some of the topics covered include</p> <ul style="list-style-type: none"> <li>• The software development life cycle</li> <li>• Security controls in software development</li> <li>• Assessing software security</li> <li>• Assessing the security implications of acquired software</li> <li>• Secure coding guidelines and standards</li> </ul>

**Table 2** Security Domains that Make Up the CISSP CBK (*continued*)

## What Does This Book Cover?

This book covers everything you need to know to become an (ISC)<sup>2</sup>-certified CISSP. It teaches you the hows and whys behind organizations' development and implementation of policies, procedures, guidelines, and standards. It covers network, application, and system vulnerabilities; what exploits them; and how to counter these threats. This book explains physical security, operational security, and why systems implement the security mechanisms they do. It also reviews the U.S. and international security criteria and evaluations performed on systems for assurance ratings, what these criteria mean, and why they are used. This book also explains the legal and liability issues that surround computer systems and the data they hold, including such subjects as computer crimes, forensics, and what should be done to properly prepare computer evidence associated with these topics for court.

While this book is mainly intended to be used as a study guide for the CISSP exam, it is also a handy reference guide for use after your certification.

## Tips for Taking the CISSP Exam

Many people feel as though the exam questions are tricky. Make sure to read each question and its answer choices thoroughly instead of reading a few words and immediately assuming you know what the question is asking. Some of the answer choices may have only subtle differences, so be patient and devote time to reading through the question more than once.

A common complaint heard about the CISSP exam is that some questions seem a bit subjective. For example, whereas it might be easy to answer a technical question that asks for the exact mechanism used in Transport Layer Security (TLS) that protects against man-in-the-middle attacks, it's not quite as easy to answer a question that asks whether an eight-foot perimeter fence provides low, medium, or high security. Many questions ask the test taker to choose the "best" approach, which some people find confusing and subjective. These complaints are mentioned here not to criticize (ISC)<sup>2</sup> and the exam writers, but to help you better prepare for the exam. This book covers all the necessary material for the exam and contains many questions and self-practice tests. Most of the questions are formatted in such a way as to better prepare you for what you will encounter on the actual exam. So, make sure to read all the material in the book, and pay close attention to the questions and their formats. Even if you know the subject well, you may still get some answers wrong—it is just part of learning how to take tests.

In answering many questions, it is important to keep in mind that some things are inherently more valuable than others. For example, the protection of human lives and welfare will almost always trump all other responses. Similarly, if all other factors are equal and you are given a choice between an expensive and complex solution and a simpler and cheaper one, the second will win most of the time. Expert advice (e.g., from an attorney) is more valuable than that offered by someone with lesser credentials. If one of the possible responses to a question is to seek or obtain advice from an expert, pay close attention to that question. The correct response may very well be to seek out that expert.



Familiarize yourself with industry standards and expand your technical knowledge and methodologies outside the boundaries of what you use today. We cannot stress enough that being the “top dog” in your particular field doesn’t mean you are properly prepared for all eight domains the exam covers.

When you take the CISSP exam at the Pearson VUE test center, other certification exams may be taking place simultaneously in the same room. Don’t feel rushed if you see others leaving the room early; they may be taking a shorter exam.

## How to Use This Book

Much effort has gone into putting all the necessary information into this book. Now it’s up to you to study and understand the material and its various concepts. To best benefit from this book, you might want to use the following study method:

- Study each chapter carefully and make sure you understand each concept presented. Many concepts must be fully understood, and glossing over a couple here and there could be detrimental to your success on the exam. The CISSP CBK contains hundreds of individual topics, so take the time needed to understand them all.
- Make sure to study and answer all of the questions. If any questions confuse you, go back and study the corresponding sections again. Remember, you will encounter questions on the actual exam that do not seem straightforward. Do not ignore the confusing questions, thinking they’re not well worded. Instead, pay even closer attention to them because they are included for a reason.
- If you are not familiar with specific topics, such as firewalls, laws, physical security, or protocol functionality, use other sources of information (books, articles, and so on) to attain a more in-depth understanding of those subjects. Don’t just rely solely on what you think you need to know to pass the CISSP exam.
- After reading this book, study the questions and answers, and take the practice tests. Then review the (ISC)<sup>2</sup> exam objectives and make sure you are comfortable with each bullet item presented. If you are not comfortable with some items, revisit the chapters in which they are covered.
- If you have taken other certification exams—such as Cisco or Microsoft—you might be used to having to memorize details and configuration parameters. But remember, the CISSP test is “an inch deep and a mile wide,” so make sure you understand the concepts of each subject *before* trying to memorize the small, specific details.
- Remember that the exam is looking for the “best” answer. On some questions test takers do not agree with any or many of the answers. You are being asked to choose the best answer out of the four being offered to you.

## PART I

# Security and Risk Management

- **Chapter 1** Cybersecurity Governance
- **Chapter 2** Risk Management
- **Chapter 3** Compliance
- **Chapter 4** Frameworks

*This page intentionally left blank*

# Cybersecurity Governance

This chapter presents the following:

- Fundamental cybersecurity concepts
- Security governance principles
- Security policies, standards, procedures, and guidelines
- Personnel security policies and procedures
- Security awareness, education, and training

---

*The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts.*

—Eugene H. Spafford

While some of us may revel in thinking about and implementing cybersecurity, the fact is that most organizations would much rather focus on many other things. Businesses exist to generate profits for their shareholders. Most nonprofit organizations are dedicated to furthering particular social causes such as charity, education, or religion. Apart from security service providers, organizations don't exist specifically to deploy and maintain firewalls, intrusion detection systems, identity management technologies, and encryption devices. No corporation really wants to develop hundreds of security policies, deploy antimalware products, maintain vulnerability management systems, constantly update its incident response capabilities, and have to comply with the myriad of security laws, regulations, and standards that exist worldwide. Business owners would like to be able to make their widgets, sell their widgets, and go home with a nice profit in their pockets. But things are not that simple.

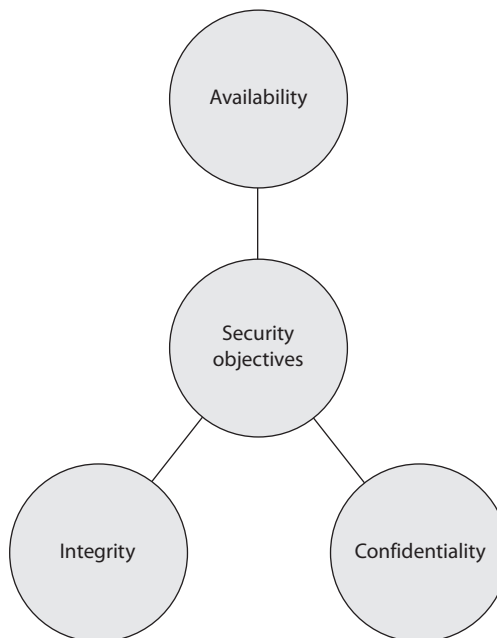
Organizations are increasingly faced with attackers who want to steal customer data to carry out identity theft and banking fraud. Company secrets are commonly being stolen by internal and external entities for economic espionage purposes. Systems are being hijacked and used within botnets to attack other organizations, mine cryptocurrencies, or spread spam. Company funds are being secretly siphoned off through complex and hard-to-identify digital methods, commonly by organized criminal rings in different countries. And organizations that find themselves in the crosshairs of attackers may come under constant attack that brings their systems and websites offline for hours or days. Companies are required to practice a wide range of security disciplines today to keep

their market share, protect their customers and bottom line, stay out of jail, and still sell their widgets.

As we start our exploration of the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) in this chapter, we will define what cybersecurity means and how it must be governed by, well, CISSPs. Each organization must develop an enterprise-wide security program that consists of technologies, procedures, and processes covered throughout this book. As you go along in your security career, you will find that most organizations have some (but rarely all) pieces to the puzzle of an “enterprise-wide security program” in place. Many of the security programs in place today can be thought of as lopsided or lumpy. The security programs excel within the disciplines that the team is most familiar with, and the other disciplines are found lacking. It is your responsibility to become as well rounded in security as possible so that you can identify these deficiencies in security programs and help improve upon them. This is why the CISSP exam covers a wide variety of technologies, methodologies, and processes—you must know and understand them holistically if you are going to help an organization carry out security holistically.

## Fundamental Cybersecurity Concepts and Terms

As cybersecurity professionals, our efforts are ultimately focused on the protection of our information systems. These systems consist of people, processes, and technologies designed to operate on information. To protect them means to ensure the confidentiality, integrity, and availability (the CIA triad) of all assets in our information systems as well as the authenticity and nonrepudiation of tasks performed in them. Each asset will require different levels of these types of protection, as we will see in the following sections.



## Confidentiality

*Confidentiality* means keeping unauthorized entities (be they people or processes) from gaining access to information assets. It ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of secrecy should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination. Confidentiality can be provided by encrypting data as it is stored and transmitted, by enforcing strict access control and data classification, and by training personnel on the proper data protection procedures.

Attackers can thwart confidentiality mechanisms by network monitoring, shoulder surfing, stealing credentials, breaking encryption schemes, and social engineering. These topics will be addressed in more depth in later chapters, but briefly, *shoulder surfing* is when a person looks over another person's shoulder and watches their keystrokes or views data as it appears on a computer screen. *Social engineering* is when one person tricks another person into sharing confidential information, for example, by posing as someone authorized to have access to that information. Social engineering can take many forms. Any one-to-one communication medium can be used to perform social engineering attacks.

Users can intentionally or accidentally disclose sensitive information by not encrypting it before sending it to another person, by falling prey to a social engineering attack, by sharing a company's trade secrets, or by not using extra care to protect confidential information when processing it.

## Integrity

*Integrity* means that an asset is free from unauthorized alterations. Only authorized entities should be able to modify an asset, and only in specific authorized ways. For example, if you are reviewing orders placed by customers on your online store, you should not be able to increase the price of any items in those orders after they have been purchased. It is your store, so you can clearly change prices as you wish. You just shouldn't be able to do it after someone agrees to buy an item at a certain price and gives you authorization to charge their credit card.

Environments that enforce and provide this attribute of security ensure that attackers, or mistakes by users, do not compromise the integrity of systems or data. When an attacker inserts malware or a back door into a system, the system's integrity is compromised. This can, in turn, harm the integrity of information held on the system by way of corruption, malicious modification, or the replacement of data with incorrect data. Strict access controls, intrusion detection, and hashing can combat these threats.

Authorized users can also affect a system or its data's integrity by mistake (although internal users may also commit malicious deeds). For example, a user with a full hard drive may unwittingly delete a configuration file under the mistaken assumption that deleting a file must be okay because the user doesn't remember ever using it. Or a user may insert incorrect values into a data-processing application that ends up charging a customer \$3,000 instead of \$300. Incorrectly modifying data kept in databases is another common way users may accidentally corrupt data—a mistake that can have lasting effects.

Security should streamline users' capabilities and give them only certain choices and functionality, so errors become less common and less devastating. System-critical files

should be restricted from viewing and access by users. Applications should provide mechanisms that check for valid and reasonable input values. Databases should let only authorized individuals modify data, and data in transit should be protected by encryption or other mechanisms.

## Availability

*Availability* protection ensures reliable and timely access to data and resources to authorized individuals. Network devices, computers, and applications should provide adequate functionality to perform in a predictable manner with an acceptable level of performance. They should be able to recover from disruptions in a secure and quick fashion, so productivity is not negatively affected. Necessary protection mechanisms must be in place to protect against inside and outside threats that could affect the availability and productivity of all business-processing components.

Like many things in life, ensuring the availability of the necessary resources within an organization sounds easier to accomplish than it really is. Networks have many pieces that must stay up and running (routers, switches, proxies, firewalls, and so on). Software has many components that must be executing in a healthy manner (operating system, applications, antimalware software, and so forth). And an organization's operations can potentially be negatively affected by environmental aspects (such as fire, flood, HVAC issues, or electrical problems), natural disasters, and physical theft or attacks. An organization must fully understand its operational environment and its availability weaknesses so that it can put in place the proper countermeasures.

## Authenticity

One of the curious features of the modern Internet is that sometimes we are unsure of who is putting out the things we read and download. Does that patch really come from Microsoft? Did your boss really send you that e-mail asking you to buy \$10,000 worth of gift cards? *Authenticity* protections ensure we can trust that something comes from its claimed source. This concept is at the heart of authentication, which establishes that an entity trying to log into a system is really who it claims to be.

Authenticity in information systems is almost always provided through cryptographic means. As an example, when you connect to your bank's website, the connection should be encrypted using Transport Layer Security (TLS), which in turn uses your bank's digital certificate to authenticate to your browser that it truly is that bank on the other end and not an impostor. When you log in, the bank takes a cryptographic hash of the credentials you provide and compares them to the hash the bank has in your records to ensure it really is you on the other end.

## Nonrepudiation

While authenticity establishes that an entity is who it claims to be at a particular point in time, it doesn't really provide historical proof of what that entity did or agreed to. For example, suppose Bob logs into his bank and then applies for a loan. He doesn't read the fine print until later, at which point he decides he doesn't like the terms of the transaction,

so he calls up the bank to say he never signed the contract and to please make it go away. Although the session was authenticated, Bob could claim that he walked away from his computer while logged into the bank's website, that his cat walked over the keyboard and stepped on ENTER, executing the transaction, and that Bob never intended to sign the loan application. It was the cat. Sadly, his claim could hold up in court.

*Nonrepudiation*, which is closely related to authenticity, means that someone cannot disavow being the source of a given action. For example, suppose Bob's bank had implemented a procedure for loan applications that required him to "sign" the application by entering his personal identification number (PIN). Now the whole cat defense falls apart unless Bob could prove he trained his cat to enter PINs.

Most commonly, nonrepudiation is provided through the use of digital signatures. Just like your physical signature on a piece of paper certifies that you either authored it or agree to whatever is written on it (e.g., a contract), the digital version attests to your sending an e-mail, writing software, or agreeing to a contract. We'll discuss digital signatures later in this book, but for now it will be helpful to remember that they are cryptographic products that, just like an old-fashioned physical signature, can be used for a variety of purposes.



**EXAM TIP** A good way to differentiate authenticity and nonrepudiation is that authenticity proves to *you* that you're talking to a given person at a given point in time. Nonrepudiation proves to *anyone* that a given person did or said something in the past.

## Balanced Security

In reality, when information security is considered, it is commonly only through the lens of keeping secrets secret (confidentiality). The integrity and availability threats tend to be overlooked and only dealt with after they are properly compromised. Some assets have a critical confidentiality requirement (e.g., company trade secrets), some have critical integrity requirements (e.g., financial transaction values), and some have critical availability requirements (e.g., e-commerce web servers). Many people understand the concepts of the CIA triad, but may not fully appreciate the complexity of implementing the necessary controls to provide all the protection these concepts cover. The following provides a *short* list of some of these controls and how they map to the components of the CIA triad.

### Availability:

- Redundant array of independent disks (RAID)
- Clustering
- Load balancing
- Redundant data and power lines
- Software and data backups



- Disk shadowing
- Co-location and offsite facilities
- Rollback functions
- Failover configurations

**Integrity:**

- Hashing (data integrity)
- Configuration management (system integrity)
- Change control (process integrity)
- Access control (physical and technical)
- Software digital signing
- Transmission cyclic redundancy check (CRC) functions

**Confidentiality:**

- Encryption for data at rest (whole disk, database encryption)
- Encryption for data in transit (IPSec, TLS, PPTP, SSH, described in Chapter 4)
- Access control (physical and technical)

All of these control types will be covered in this book. What is important to realize at this point is that while the concept of the CIA triad may seem simplistic, meeting its requirements is commonly more challenging.

## Other Security Terms

The words “vulnerability,” “threat,” “risk,” and “exposure” are often interchanged, even though they have different meanings. It is important to understand each word’s definition and the relationships between the concepts they represent.

A *vulnerability* is a weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

A *threat* is any potential danger that is associated with the exploitation of a vulnerability. If the threat is that someone will identify a specific vulnerability and use it against the organization or individual, then the entity that takes advantage of a vulnerability is referred to as a *threat agent* (or *threat actor*). A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy, or an employee circumventing controls in order to copy files to a medium that could expose confidential information.

A *risk* is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact. If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method. If users are not educated on processes and procedures, there is a higher likelihood that an employee will make an unintentional mistake that may destroy data. If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

An *exposure* is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages. If password management is lax and password rules are not enforced, the organization is exposed to the possibility of having users' passwords compromised and used in an unauthorized manner. If an organization does not have its wiring inspected and does not put proactive fire prevention steps into place, it exposes itself to potentially devastating fires.

A *control*, or *countermeasure*, is put into place to mitigate (reduce) the potential risk. A countermeasure may be a software configuration, a hardware device, or a procedure that eliminates a vulnerability or that reduces the likelihood a threat agent will be able to exploit a vulnerability. Examples of countermeasures include strong password management, firewalls, a security guard, access control mechanisms, encryption, and security awareness training.



**NOTE** The terms “control,” “countermeasure,” and “safeguard” are interchangeable terms. They are mechanisms put into place to reduce risk.

If an organization has antimalware software but does not keep the signatures up to date, this is a vulnerability. The organization is vulnerable to more recent malware attacks. The threat is that a threat agent will insert malware into the environment and disrupt productivity. The risk is the likelihood of a threat agent using malware in the environment and the resulting potential damage. If this happens, then a vulnerability has been exploited and the organization is exposed to loss. The countermeasures in this situation are to update the signatures and install the antimalware software on all computers. The relationships among risks, vulnerabilities, threats, and countermeasures are shown in Figure 1-1.

Applying the right countermeasure can eliminate the vulnerability and exposure, and thus reduce the risk. The organization cannot eliminate the threat agent, but it can protect itself and prevent this threat agent from exploiting vulnerabilities within the environment.

Many people gloss over these basic terms with the idea that they are not as important as the sexier things in information security. But you will find that unless a security team has an agreed-upon language in place, confusion will quickly take over. These terms embrace the core concepts of security, and if they are confused in any manner, then the activities that are rolled out to enforce security are commonly confused.