LEARNING MADE EASY

8th Edition

CISSP®

for dummies®

A Wiley Brand

WITH ONLINE PRACTICE

FEATURES

300+ Study Questions

Digital Flashcards

Expert Strategies

Lawrence C. Miller, CISSP

Peter H. Gregory, CISSP

This book comes with access to more content online.

Quiz yourself and study
with flashcards!

Register your book or ebook at
www.dummies.com/go/getaccess.

Select your product, and then follow the prompts
to validate your purchase.

You'll receive an email with your PIN and instructions.

CISSP®

8th Edition

by Lawrence C. Miller, CISSP and
Peter H. Gregory, CISSP

for dummies®
A Wiley Brand

CISSP® For Dummies®, 8th Edition

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Copyright © 2024 by John Wiley & Sons, Inc. All rights reserved, including rights for text and data mining and training of artificial technologies or similar technologies.

Media and software compilation copyright © 2024 by John Wiley & Sons, Inc. All rights reserved, including rights for text and data mining and training of artificial technologies or similar technologies.

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc., and may not be used without written permission. CISSP is a registered certification mark of ISC2, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHOR HAVE USED THEIR BEST EFFORTS IN PREPARING THIS BOOK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS BOOK AND SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. THE ADVISE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A PROFESSIONAL WHERE APPROPRIATE. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit https://hub.wiley.com/community/support/dummies.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2024939385

ISBN 978-1-394-26177-2 (pbk); ISBN 978-1-394-26178-9 (ebk); ISBN 978-1-394-26179-6 (ebk)

Contents at a Glance

Introduction 1

Part 1: Getting Started with CISSP Certification 7

CHAPTER 1: ISC2 and the CISSP Certification 9

CHAPTER 2: Putting Your Certification to Good Use 23

Part 2: Certification Domains 43

CHAPTER 3: Security and Risk Management 45

CHAPTER 4: Asset Security 141

CHAPTER 5: Security Architecture and Engineering 167

CHAPTER 6: Communication and Network Security 269

CHAPTER 7: Identity and Access Management 323

CHAPTER 8: Security Assessment and Testing 365

CHAPTER 9: Security Operations 395

CHAPTER 10: Software Development Security 459

Part 3: The Part of Tens 493

CHAPTER 11: Ten Ways to Prepare for the Exam 495

CHAPTER 12: Ten Test-Day Tips 501

Glossary 505

Index 561

Table of Contents

INTRODUCTION 1
About This Book. 2
Foolish Assumptions. 3
Icons Used in This Book 3
Beyond the Book 4
Where to Go from Here 5

PART 1: GETTING STARTED WITH CISSP CERTIFICATION 7

CHAPTER 1: ISC2 and the CISSP Certification 9
You Must Be This Tall to Ride This Ride (And Other Requirements). 10
Preparing for the Exam 12
Studying on your own. 12
Getting hands-on experience 13
Getting official ISC2 CISSP training 14
Attending other training courses or study groups 15
Taking practice exams 15
Are you ready for the exam? 15
Registering for the Exam 16
About the CISSP Examination 17
After the Examination. 20

CHAPTER 2: Putting Your Certification to Good Use. 23
Networking with Other Security Professionals 24
Being an Active ISC2 Member 25
Considering ISC2 Volunteer Opportunities 26
Writing certification exam questions 27
Speaking at events 27
Helping at ISC2 conferences 27
Reading and contributing to ISC2 publications. 27
Supporting the ISC2 Center for Cyber Safety and Education 28
Participating in bug-bounty programs 28
Participating in ISC2 focus groups 28
Joining the ISC2 community. 28
Getting involved with a CISSP study group 28
Becoming an Active Member of Your Local Security Chapter 29
Spreading the Good Word about CISSP Certification. 30

Helping Others 31
Using Your CISSP Certification to Be an Agent of Change 33
Earning Other Certifications 34
Other ISC2 certifications 34
CISSP concentrations 35
Non-ISC2 certifications 35
Choosing the right certifications 39
Building your professional brand 40
Pursuing Security Excellence 42

PART 2: CERTIFICATION DOMAINS 43

CHAPTER 3: Security and Risk Management 45
Understand, Adhere to, and Promote Professional Ethics 46
ISC2 Code of Professional Ethics 47
Organizational code of ethics 48
Understand and Apply Security Concepts 50
Confidentiality 51
Integrity 52
Availability 52
Authenticity 53
Nonrepudiation 54
Evaluate, Apply, and Sustain Security Governance Principles 54
Alignment of the security function to business strategy, goals, mission, and objectives 54
Organizational processes 55
Organizational roles and responsibilities 57
Security control frameworks 58
Due care and due diligence 62
Understand Legal, Regulatory, and Compliance Issues That Pertain to Information Security 63
Cybercrimes and data breaches 64
Licensing and intellectual property requirements 77
Import/export controls 80
Transborder data flow 80
Issues related to privacy 81
Contractual, legal, industry standards, and regulatory requirements 88
Understand Requirements for Investigation Types 91
Develop, Document, and Implement Security Policies, Standards, Procedures, and Guidelines 93
Policies 93
Standards (and baselines) 94

Procedures 95
Processes 95
Guidelines. 95
Identify, Analyze, Assess, Prioritize, and Implement Business Continuity (BC) Requirements. 95
Business impact analysis 98
External dependencies 106
Contribute to and Enforce Personnel Security Policies and Procedures 108
Candidate screening and hiring 108
Employment agreements and policy-driven requirements 111
Onboarding, transfers, and termination processes 111
Vendor, consultant, and contractor agreements and controls. . .112
Understand and Apply Risk Management Concepts 113
Threat and vulnerability identification 113
Risk analysis, assessment, and scope. 114
Risk response and treatment 120
Applicable types of controls. 121
Control assessments (security and privacy) 124
Continuous monitoring and measurement. 127
Reporting 127
Continuous improvement 128
Risk frameworks 128
Understand and Apply Threat Modeling Concepts and Methodologies. 130
Identifying threats 131
Determining and diagramming potential attacks. 131
Performing reduction analysis 132
Remediating threats 132
Threat hunting 133
Apply Supply Chain Risk Management (SCRM) Concepts 134
Risks associated with the acquisition of products and services from suppliers and providers. 135
Risk mitigations 135
Establish and Maintain a Security Awareness, Education, and Training Program. 137
Methods and techniques to increase awareness and training. . .137
Periodic content reviews to include emerging technologies and trends. 140
Program effectiveness evaluation. 140

CHAPTER 4: **Asset Security** 141
Identify and Classify Information and Assets 142
Data classification 145
Asset classification. 149

Establish Information and Asset Handling Requirements 150
Provision Information and Assets Securely. 152
Information and asset ownership. 152
Asset inventory 154
Asset management 155
Manage Data Life Cycle 155
Data roles 156
Data collection 157
Data location 157
Data maintenance. 157
Data retention 158
Data remanence 159
Data destruction 159
Ensure Appropriate Asset Retention 159
End of life 160
End of support 160
Determine Data Security Controls and Compliance Requirements. 161
Data states 161
Scoping and tailoring 163
Standards selection. 163
Data protection methods 164

CHAPTER 5: **Security Architecture and Engineering** 167
Using Secure Design Principles in Engineering Processes 168
Threat modeling 169
Least privilege 172
Defense in depth 175
Secure defaults 175
Fail securely 176
Segregation of duties (SoD) 176
Keep it simple and small. 176
Zero trust or trust but verify 177
Privacy by design 179
Shared responsibility 180
Secure access service edge (SASE) 183
Understand the Fundamental Concepts of Security Models 184
Select Controls Based Upon Systems Security Requirements 187
Evaluation criteria 188
System certification and accreditation. 194
Understand Security Capabilities of Information Systems 196
Memory protection 196
Trusted Computing Base 196
Trusted Platform Module 197

Hardware Security Module (HSM) 197
Secure modes of operation 198
Open and closed systems 198
Encryption and decryption 199
Protection rings 199
Security modes 200
Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements 200
Client-based systems 202
Server-based systems 203
Database systems 203
Cryptographic systems 203
Operational technology/industrial control systems 204
Cloud-based systems 205
Distributed systems 208
Internet of Things 209
Microservices 209
Containerization 210
Serverless 211
Embedded systems 212
High-performance computing systems 213
Edge computing systems 213
Virtualized systems 214
Web-based systems 215
Mobile systems 216
Select and Determine Cryptographic Solutions 217
Plaintext and ciphertext 218
Encryption and decryption 218
End-to-end encryption 218
Link encryption 219
Putting it all together: The cryptosystem .220
Classes of ciphers 221
Types of ciphers 223
Cryptographic life cycle 225
Cryptographic methods 226
Public key infrastructure 236
Key management practices 237
Digital signatures and digital certificates 238
Nonrepudiation 239
Integrity (hashing) 239
Understand Methods of Cryptanalytic Attacks 242
Brute force 242
Ciphertext only 243
Known plaintext 243

Frequency analysis 243
Chosen ciphertext 243
Implementation attacks 244
Side channel 244
Fault injection. 244
Timing 245
Man in the middle 245
Pass the hash 245
Kerberos exploitation 245
Rubber hose 246
Ransomware 246
Apply Security Principles to Site and Facility Design 247
Design Site and Facility Security Controls 250
Wiring closets/intermediate distribution frames 253
Server rooms/data centers 253
Media storage facilities. 254
Evidence storage 254
Restricted and work area security. 255
Utilities and heating, ventilation, and air conditioning 256
Environmental issues 257
Fire prevention, detection, and suppression. 258
Power 262
Manage the Information System Lifecycle. 264
Inception 264
Stakeholder needs and requirements 265
Requirements analysis 265
Architectural design 265
Development/Implementation 265
Integration 266
Verification and validation 266
Transition/deployment. 267
Operations and maintenance/sustainment 267
Retirement/disposal 267

CHAPTER 6: **Communication and Network Security** 269
Apply Secure Design Principles in Network Architectures 270
Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models 270
Internet Protocol (IP) version 4 and 6. 284
Secure protocols 289
Implications of multilayer protocols. 291
Converged protocols. 291

Transport architecture 292
Performance metrics 294
Traffic flows 294
Physical segmentation 295
Logical segmentation 295
Microsegmentation 296
Edge networks 296
Wireless networks 297
Cellular/mobile networks 299
Content distribution networks (CDN) 300
Software-defined networks (SDN) 301
Virtual private cloud (VPC) 303
Monitoring and management 303
Secure Network Components 303
Operation of infrastructure 303
Transmission media 304
Network access control (NAC) systems 306
Endpoint security. 316
Implement Secure Communication Channels According to Design. 318
Voice, video, and collaboration 318
Remote access 320
Data communications. 322
Third-party connectivity 322

CHAPTER 7: **Identity and Access Management** 323
Control Physical and Logical Access to Assets 324
Information 324
Systems. 324
Devices 325
Facilities. 326
Applications 327
Services 327
Design Identification and Authentication Strategy. 328
Groups and roles. 328
Authentication, authorization, and accounting. 329
Session management 344
Registration, proofing, and establishment of identity 345
Federated identity management. 346
Credential management systems 347
Single sign-on. 347
Just-in-time 348

Federated Identity with a Third-Party Service .348
On-premises 350
Cloud 350
Hybrid 350
Implement and Manage Authorization Mechanisms 351
Role-based access control 351
Rule-based access control 352
Mandatory access control 352
Discretionary access control 353
Attribute-based access control 354
Risk-based access control 355
Access policy enforcement. 355
Manage the Identity and Access Provisioning Lifecycle 355
Account access review 356
Provisioning and deprovisioning. 356
Role definition and transition 357
Privilege escalation 357
Service accounts management 357
Implement Authentication Systems 358
OpenID Connect/Open Authorization 359
Security Assertion Markup Language 359
Kerberos 359
RADIUS and TACACS+ 363

CHAPTER 8: **Security Assessment and Testing** 365
Design and Validate Assessment, Test, and Audit Strategies 366
Conduct Security Control Testing 367
Vulnerability assessment 367
Penetration testing 370
Log reviews. 374
Synthetic transactions. 377
Code review and testing 377
Misuse case testing 378
Test coverage analysis 379
Interface testing. 379
Breach and attack simulations 380
Compliance checks 380
Collect Security Process Data 381
Account management. 382
Management review and approval 383
Key performance and risk indicators 383
Backup verification data 385

Training and awareness 386
Disaster recovery and business continuity 387
Analyze Test Output and Generate Reports 388
Remediation 388
Exception handling 390
Ethical disclosure 390
Conduct or Facilitate Security Audits 391
CHAPTER 9: **Security Operations** 395
Understand and Comply with Investigations .396
Evidence collection and handling 396
Reporting and documentation 403
Investigative techniques 404
Digital forensics tools, tactics, and procedures. 406
Artifacts 407
Conduct Logging and Monitoring Activities. .407
Intrusion detection and prevention system (IDPS). 407
Security information and event management (SIEM) 409
Security orchestration, automation, and response (SOAR). 409
Continuous monitoring and tuning 410
Egress monitoring 410
Log management. 411
Threat intelligence. 411
User and entity behavior analytics 412
Perform Configuration Management (CM) 412
Apply Foundational Security Operations Concepts 414
Need to know and least privilege 415
Segregation of duties and responsibilities. 416
Privileged account management. 417
Job rotation. 419
Service-level agreements 421
Apply Resource Protection. 424
Media management 424
Media protection techniques. 426
Data at rest/data in transit. 426
Conduct Incident Management. 427
Detection 428
Response 428
Mitigation 428
Reporting 428
Recovery 429
Remediation. 429
Lessons learned. 429

Operate and Maintain Detective and Preventive Measures 429
- Firewalls 430
- Intrusion detection systems (IDS) and intrusion prevention systems (IPS) 430
- Allow (or permit) list and block (or deny) list 430
- Third-party provided security services 430
- Sandboxing 431
- Honeypots/honeynets 431
- Anti-malware 431
- Machine learning and artificial intelligence (AI) based tools 432
- Performance management 432

Implement and Support Patch and Vulnerability Management 432

Understand and Participate in Change Management Processes 433

Implement Recovery Strategies 434
- Backup storage strategies 434
- Recovery site strategies 437
- Multiple processing sites 439
- System resilience, high availability (HA), quality of service (QoS), and fault tolerance 439

Implement Disaster Recovery (DR) Processes 441
- Response 445
- Personnel 447
- Communications 448
- Assessment 449
- Restoration 449
- Training and awareness 450
- Lessons learned 450

Test Disaster Recovery Plans 450
- Read-through/tabletop 451
- Walkthrough 451
- Simulation 452
- Parallel 453
- Full interruption 453

Participate in Business Continuity Planning and Exercises 454

Implement and Manage Physical Security 456
- Perimeter security controls 457
- Internal security controls 457

Address Personnel Safety and Security Concerns 457
- Travel 457
- Security training and awareness 458
- Emergency management 458
- Duress 458

CHAPTER 10: **Software Development Security** 459
Understand and Integrate Security in the Software Development Life Cycle 460
Development methodologies 460
Maturity models. 469
Operation and maintenance 470
Change management 471
Integrated product team 472
Identify and Apply Security Controls in Software Development Ecosystems 472
Programming languages 473
Libraries 474
Tool sets 474
Integrated development environment. 476
Runtime. 476
Continuous integration/continuous delivery. 477
Security orchestration, automation, and response 477
Software configuration management 478
Code repositories 479
Application security testing 480
Assess the Effectiveness of Software Security 482
Auditing and logging of changes 483
Risk analysis and mitigation. 483
Assess the Security Impact of Acquired Software 485
Define and Apply Secure Coding Guidelines and Standards 487
Security weaknesses and vulnerabilities at the source-code level. 487
Security of application programming interfaces 488
Secure coding practices 489
Software-defined security 491

PART 3: THE PART OF TENS. 493

CHAPTER 11: **Ten Ways to Prepare for the Exam** 495
Know Your Learning Style 495
Get a Networking Certification First 496
Register Now 496
Make a 60-Day Study Plan 496
Get Organized and Read 497
Join a Study Group. 497
Take Practice Exams 498
Take a CISSP Training Seminar 498
Adopt an Exam-Taking Strategy 498
Take a Breather 499

CHAPTER 12: **Ten Test-Day Tips** 501
Get a Good Night's Rest 501
Dress Comfortably 502
Eat a Good Meal. 502
Arrive Early 502
Bring Approved Identification 502
Bring Snacks and Drinks. 503
Bring Prescription and Over-the-Counter Medications 503
Leave Your Mobile Devices Behind. 503
Take Frequent Breaks. 504
Guess — As a Last Resort. 504

GLOSSARY. 505

INDEX. 561

Introduction

Since 1994, security practitioners around the world have been pursuing a well-known and highly regarded professional credential: the Certified Information Systems Security Professional (CISSP) certification. At 30 years of age, CISSP is one of the oldest and most respected cybersecurity certifications in existence. And since 2001, *CISSP For Dummies* has been helping security practitioners enhance their security knowledge and earn the coveted CISSP certification.

Today, there are approximately 156,000 CISSPs worldwide. Ironically, some skeptics might argue that the CISSP certification is becoming less relevant because so many people have earned it. But the CISSP certification isn't less relevant because more people are attaining it; more people are attaining it because it's more relevant now than ever. Information security is far more important than ever, with extremely large-scale data security breaches and highly sophisticated cyberattacks becoming all too frequent in our modern era. And many countries are passing more laws and regulations concerning information security and security breaches.

Many excellent and reputable information security training and education programs are available. In addition to technical and industry certifications, many fully accredited postsecondary degrees, certificates, and apprenticeship programs are available for information security practitioners. And certainly, plenty of self-taught, highly skilled people are working in the information security field who have a strong understanding of core security concepts, techniques, and technologies. But inevitably, too many charlatans are all too willing to overstate their security qualifications, preying on the obliviousness of business and other leaders to pursue a fulfilling career in the information security field (or for other, more dubious purposes).

The CISSP certification is widely regarded as *the* professional standard for information security professionals. It enables security professionals to distinguish themselves from others by validating *both* their knowledge and experience. Likewise, it enables businesses and other organizations to identify qualified information security professionals and verify the knowledge and experience of candidates for critical information security roles in their organizations. Thus, the CISSP certification is more relevant and important than ever.

About This Book

Some say that a CISSP candidate requires a breadth of knowledge many miles across but only a few inches deep. To embellish on this statement, we believe that a CISSP candidate is more like the Great Wall of China, with a knowledge base extending over 3,500 miles — with maybe a few holes here and there, stronger in some areas than others, but nonetheless one of the Seven Wonders of the Modern World.

The problem with lots of CISSP preparation materials is defining how high (or deep) the Great Wall is. Some material overwhelms and intimidates CISSP candidates, leading them to believe that the wall is as high as it is long. Other study materials are perilously brief and shallow, giving the unsuspecting candidate a false sense of confidence while attempting to step over the Great Wall, careful not to stub a toe. To help you avoid either misstep, *CISSP For Dummies,* 8th Edition, answers the question "What level of knowledge and experience must a CISSP candidate possess to succeed on the CISSP exam?"

Our goal in this book is simple: to help you prepare for and pass the CISSP examination so that you can join the ranks of respected certified security professionals who dutifully serve and protect organizations and industries around the world. Although we've stuffed this book chock-full of good information, we don't expect it to be a weighty desktop reference on the shelf of every security professional — although we certainly wouldn't object.

Also, we don't intend this book to be an all-purpose, be-all-and-end-all, one-stop shop with all the answers to life's great mysteries. Given the broad base of knowledge required for the CISSP certification, we strongly recommend that you use multiple resources to prepare for the exam and study as much relevant information as your time and resources allow. *CISSP For Dummies,* 8th Edition, provides the framework and the blueprint for your study effort and sufficient information to help you pass the exam, but by itself, it won't make you an information security expert. That takes knowledge, skills, and on-the-job experience!

Finally, as a security professional, earning your CISSP certification is only the beginning. Business and technology, which have associated risks and vulnerabilities, require us, as security professionals, to press forward constantly, consuming vast volumes of knowledge and information in a constant tug-of-war against our adversaries — lone wolves, cybercriminal organizations, and well-funded nation-states. Earning your CISSP is an outstanding achievement and an essential hallmark in a lifetime of continuous learning.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but we assume a few things nonetheless! Mainly, we assume that

- **You have at least five years of professional experience in two or more of the eight domains covered on the CISSP exam** (corresponding to Chapters 3 through 10 of this book). Actually, this is more than an assumption; it's a requirement for CISSP certification. Even if you lack the minimum experience, however, some experience waivers are available for certain certifications and college education (we cover the specifics in Chapter 1), and you can still take the CISSP exam and apply for certification after you meet the experience requirement.
- **You have general IT experience — perhaps even many years of experience.** Passing the CISSP exam requires considerable knowledge of information security and underlying IT technologies and fundamentals such as networks, operating systems, and programming.
- **You have access to the Internet.** Throughout this book, we provide lots of URLs for websites about technologies, standards, laws, tools, security associations, and other certifications that you'll find helpful as you prepare for the CISSP exam. And chances are, you'll be curious about the topics we discuss and go online to learn even more.
- **You are a white hat security professional.** By *white hat,* we mean that you act lawfully and will have no problem abiding by the ISC2 Code of Ethics (which is a requirement for CISSP certification).

Icons Used in This Book

Throughout this book, you occasionally see icons in the margin that call attention to important information that's particularly worth noting. You won't see smiley faces winking at you or any other cute little emoticons, but you'll definitely want to take note! Here's what to look for and what to expect.

CROSS REFERENCE

This icon identifies the CISSP Common Body of Knowledge (CBK) objective covered in each section.

REMEMBER

This icon identifies general information and core concepts that are well worth committing to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries, birthdays, and other important events. You should certainly understand and review this information before taking the CISSP exam.

TIP

Tips are never expected but always appreciated, and we sure hope you'll appreciate these tips! This icon flags helpful suggestions and tidbits of useful information that may save you time and headaches.

WARNING

This icon marks the stuff your mother warned you about. Well, okay, probably not, but you should take heed nonetheless. These helpful alerts point out confusing or difficult-to-understand terms and concepts.

TECHNICAL STUFF

You won't find a map of the human genome or the secret to cold fusion in this book (or maybe you will), but if you're an insufferable insomniac, take note. This icon explains the jargon beneath the jargon and is the stuff that legends — or at least nerds — are made of. So, if you're seeking to attain the seventh level of *nerd*-vana, keep an eye out for these icons!

Beyond the Book

In addition to what you're reading right now, this book comes with a free, access-anywhere Cheat Sheet that includes tips to help you prepare for the CISSP exam and your date with destiny (your exam day). To get this Cheat Sheet, simply go to `www.dummies.com` and type **CISSP For Dummies Cheat Sheet** in the Search box.

You also get access to hundreds of practice CISSP exam questions and dozens of flash cards. Use the exam questions to identify specific topics and domains that you may need to spend a little more time studying and to become familiar with the types of questions you'll encounter on the CISSP exam (including multiple-choice, drag-and-drop, and hotspot). To gain access to the online practice material, all you have to do is register. Just follow these simple steps:

1. **Register your book or e-book at `Dummies.com` to get your personal identification number (PIN).**

   Go to `www.dummies.com/go/getaccess`.

2. **Choose your product from the drop-down list on that page.**
3. **Follow the prompts to validate your product.**

4. **Check your email for a confirmation message that includes your PIN and instructions for logging in.**

   If you don't receive this email within two hours, please check your spam folder before contacting us through our support website at `https://support.wiley.com` or by phone at +1 (877) 762-2974.

Now you're ready to go! You can come back to the practice material as often as you want. Simply log in with the username and password you created during your initial login; you don't need to enter the access code a second time.

Your registration is good for one year from the day you activate your PIN.

Where to Go from Here

If you don't know where you're going, any chapter will get you there, but Chapter 1 may be a good place to start. If you see a particular topic that piques your interest, however, feel free to jump ahead to that chapter. Each chapter is individually wrapped (but not packaged for individual sale) and written to stand on its own, so feel free to start reading anywhere and skip around! Read this book in any order that suits you (though we don't recommend upside down or backward).

1

Getting Started with CISSP Certification

IN THIS PART . . .

Get acquainted with ISC2 and the CISSP certification.

Advance your security career as a CISSP.

IN THIS CHAPTER

- » Learning about ISC2 and the CISSP certification
- » Understanding CISSP certification requirements
- » Developing a study plan
- » Registering for the exam
- » Taking the CISSP exam
- » Getting your exam results

Chapter 1

ISC2 and the CISSP Certification

In this chapter, you get to know the ISC2 and learn about the CISSP certification, including professional requirements, how to study for the exam, how to get registered, what to expect during the exam, and (of course) what to expect after you pass the CISSP exam!

The International Information System Security Certification Consortium, or ISC2, (`www.isc2.org`) was established in 1989 as a not-for-profit, tax-exempt corporation chartered for the explicit purpose of developing a standardized security curriculum and administering an information security certification process for security professionals worldwide. In 1994, the Certified Information Systems Security Professional (CISSP) credential was launched.

The CISSP was the first information security credential accredited by the American National Standards Institute (ANSI) to the ISO/IEC 17024 standard. This international standard helps ensure that personnel certification processes define specific competencies and identify required knowledge, skills, and personal attributes. It also requires examinations to be independently administered and designed to properly test a candidate's competence for the certification.

This process helps a certification gain industry acceptance and credibility as more than just a marketing tool for certain vendor-specific certifications (a widespread criticism that has diminished the popularity of many vendor certifications over the years).

TECHNICAL STUFF

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are two organizations that work together to prepare and publish international standards for businesses, governments, and societies worldwide.

The CISSP certification is based on a Common Body of Knowledge (CBK) identified by the ISC2 and defined through eight distinct domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

You Must Be This Tall to Ride This Ride (And Other Requirements)

The CISSP candidate must have a minimum of the equivalent of five cumulative years of professional (paid), *full-time*, direct work experience in two or more of the domains listed in the preceding section. Full-time experience is accrued monthly and requires full-time employment for a minimum of 35 hours per week and 4 weeks per month to get credit for 1 month of full-time work experience. Part-time experience can also be credited if you are employed fewer than 35 hours per week but at least 20 hours per week; 1,040 hours of part-time experience would be the equivalent of 6 months of full-time experience. Credit for work experience can also be earned for paid or unpaid internships. You'll need documentation from the organization confirming your experience or from the registrar if you're interning at a school.