(ISC)²®

SSCP® Systems Security Certified Practitioner

Official Study Guide

Second Edition

(ISC)²®

SSCP® Systems Security Certified Practitioner

Official Study Guide

Second Edition

Mike Wills

SYBEX®
A Wiley Brand

Development Editor: Kim Wimpsett
Technical Editor: Scott Pike
Production Editor: Lauren Freestone
Copy Editor: Elizabeth Welch
Editorial Manager: Pete Gaughan
Production Manager: Kathleen Wisor
Associate Publisher: Jim Minatel
Proofreader: Tiffany Taylor
Indexer: Johnna VanHoose Dinse
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: © Getty Images Inc./Jeremy Woodhouse

Published simultaneously in Canada

ISBN: 978-1-119-54294-0
ISBN: 978-1-119-54295-7 (ebk.)
ISBN: 978-1-119-54292-6 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2019936132

10 9 8 7 6 5 4 3 2 1

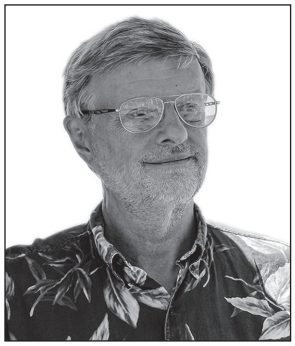
Acknowledgments

This book owes a great deal to the many teachers, coworkers, teammates, and friends who've worked so hard for so long to teach me what I know about information security and insecurity, and about risk management and mismanagement. Where this book works well in conveying that body of knowledge, skills, and attitudes to you is a testament to their generosity in sharing their insights with me. I would also like to acknowledge my faculty teammates here at Embry-Riddle Aeronautical University for sharing their frank and candid views throughout many conversations on making this body of knowledge accessible and engaging in the classroom. The ideas and experiences of Dr. Aaron Glassman, Dr. Wesley Phillips, Dr. Robert "Trez" Jones, and Mr. Hamid Ait Kaci Azzou have profoundly affected my approach to what you see before you here in this book.

The combined team at Wiley/Sybex and at $(ISC)^2$ worked tirelessly to focus, strengthen, and clarify what I wanted to say and how I said it, all while keeping my voice and my teaching ideas authentic and on point. My thanks go out to the editorial team at Wiley/Sybex: Jim Minatel, Kim Wimpsett, Pete Gaughan, Lauren Freestone, Elizabeth Welch, Tiffany Taylor, and their technical reviewers Jacob Penovich, Scott Pike, and Raven Sims, as well as to Tara Zeiler and Charles Gaughf, our reviewers at $(ISC)^2$. Johnna VanHoose Dinse, Wiley's indexer, has also made the art of finding what you want in this book when you need it more of a science (and I've always had a soft spot for a great index!). Where this book works well for you, it works because of the efforts of all of those people to make this book the best it can be. What errors, omissions, misspeaks, and confusions that remain are mine, not theirs.

Finally, I wish to thank my wife Nancy. She saved my life and brought me peace. Her strength inspired me to say "yes" when Jim first called me about doing this book and has kept both of us healthy and happy throughout.

About the Author



Mike Wills, SSCP, CISSP has spent more than 40 years as a computer systems architect, programmer, security specialist, database designer, consultant, and teacher (among other duties). Starting out as a bit of a phone phreak in his college days, he sharpened his skills on the 1960s generation of mainframes and minicomputers, just in time for the first 8080 and Z80 microprocessors to fuel the home computer revolution. Learning about the ARPANET just added spice to that mix. Since then, he's had ones, zeros, and now qubits under his fingernails too many times to count, whether as part of his jobs, his teaching, or his hobbies.

Mike earned his BS and MS degrees in computer science, both with minors in electrical engineering, from Illinois Institute of Technology, and his MA in Defence Studies from King's College, London. He is a graduate of the Federal Chief Information Officer program at National Defense University and the Program Manager's Course at Defense Systems Management College.

As an Air Force officer, Mike served in the National Reconnaissance Office, building and flying some of the most complex, cutting-edge space-based missions, large and small. As a "ground control" guy, he specialized in the design, operation, and support of highly secure, globe-spanning command, control, communications, and intelligence systems that support US and Coalition missions around the world. These duties often required Mike to "optimize" his way around the official configuration management and security safeguards—all on official business, of course.

No good deed going unpunished, he then spent two years on the Joint Staff as a policy and budget broker for all command, control, and communications systems, and then taught in the School of Information Warfare and Strategy at National Defense University. He's taught at senior leader colleges in both the United States and United Kingdom, and has been a continuing guest lecturer at the UK's Defence Academy. He served as adviser to the UK's Joint Intelligence Committee, Ministry of Justice, and Defence Science and Technology Laboratories on the national and personal security implications of science and technology policy; this led to him sometimes being known as the UK's nonresident expert on outer space law.

Currently he is an assistant professor of Applied Information Technologies in the College of Business at Embry-Riddle Aeronautical University – Worldwide, where he is the change leader and academic visionary behind bringing the Microsoft Software and Systems Academy program into ERAU's classrooms at 13 locations around the United States. Prior to this, Mike helped create two new MS degrees—Information Security and Assurance, and Management of Information Systems—and was program chair of both during their launch and first year of teaching. He also taught in Worldwide's Security and Intelligence Studies program during its 2005 launch in ERAU's European Division.

Mike and his wife Nancy currently call Montevideo, Uruguay, their home. Living abroad since the end of the last century, they find new perspectives, shared values, and wonderful people wherever they go. As true digital nomads, it's getting time to move again. Where to? They'll find out when they get there.

Contents at a Glance

Foreword		*xxi*
Introduction		*xxiii*
Self-Assessment		*xlv*
Part I	**Getting Started as an SSCP**	**1**
Chapter 1	The Business Case for Decision Assurance and Information Security	3
Chapter 2	Information Security Fundamentals	25
Part II	**Integrated Risk Management and Mitigation**	**51**
Chapter 3	Integrated Information Risk Management	53
Chapter 4	Operationalizing Risk Mitigation	111
Part III	**The Technologies of Information Security**	**173**
Chapter 5	Communications and Network Security	175
Chapter 6	Identity and Access Control	249
Chapter 7	Cryptography	297
Chapter 8	Hardware and Systems Security	371
Chapter 9	Applications, Data, and Cloud Security	413
Part IV	**People Power: What Makes or Breaks Information Security**	**477**
Chapter 10	Incident Response and Recovery	479
Chapter 11	Business Continuity via Information Security and People Power	525
Chapter 12	Risks, Issues, and Opportunities, Starting Tomorrow	553
Appendix	Answers to Review Questions	569
Index		*605*

Contents

Foreword *xxi*

Introduction *xxiii*

Self-Assessment *xlv*

Part I Getting Started as an SSCP 1

Chapter 1 The Business Case for Decision Assurance and Information Security 3

Information: The Lifeblood of Business 4
Data, Information, Knowledge, Wisdom… 5
Information Is *Not* Information Technology 8
Policy, Procedure, and Process: How Business Gets Business Done 10
Who Is the Business? 11
"What's Your Business Plan?" 12
Purpose, Intent, Goals, Objectives 13
Business Logic and Business Processes: Transforming Assets into Opportunity, Wealth, and Success 14
The Value Chain 15
Being Accountable 17
Who Runs the Business? 19
Owners and Investors 19
Boards of Directors 20
Managing or Executive Directors and the "C-Suite" 20
Layers of Function, Structure, Management, and Responsibility 21
Plans and Budgets, Policies, and Directives 22
Summary 23

Chapter 2 Information Security Fundamentals 25

The Common Needs for Privacy, Confidentiality, Integrity, and Availability 26
Privacy 26
Confidentiality 29
Integrity 30
Availability 31
Privacy vs. Security, or Privacy and Security? 32
CIA Needs of Individuals 34

Private Business's Need for CIA 35
Government's Need for CIA 36
The Modern Military's Need for CIA 36
Do Societies Need CIA? 36
Training and Educating Everybody 38
SSCPs and Professional Ethics 38
Summary 40
Exam Essentials 40
Review Questions 44

Part II Integrated Risk Management and Mitigation 51

Chapter 3 Integrated Information Risk Management 53

It's a Dangerous World 54
What Is Risk? 55
Risk: When Surprise Becomes Disruption 59
Information Security: Delivering Decision Assurance 60
"Common Sense" and Risk Management 63
The Four Faces of Risk 65
Outcomes-Based Risk 67
Process-Based Risk 67
Asset-Based Risk 68
Threat-Based (or Vulnerability-Based) Risk 69
Getting Integrated and Proactive with Information Defense 72
Trust, but Verify 76
Due Care and Due Diligence: Whose Jobs Are These? 76
Be Prepared: First, Set Priorities 77
Risk Management: Concepts and Frameworks 78
The SSCP and Risk Management 81
Plan, Do, Check, Act 82
Risk Assessment 84
Establish Consensus about Information Risk 84
Information Risk Impact Assessment 85
The Business Impact Analysis 92
From Assessments to Information Security Requirements 92
Four Choices for Limiting or Containing Damage 94
Deter 96
Detect 96
Prevent 97
Avoid 97
Summary 100
Exam Essentials 101
Review Questions 105

Chapter 4 Operationalizing Risk Mitigation 111

From Tactical Planning to Information Security Operations 112
Operationally Outthinking Your Adversaries 114
Getting Inside the Other Side's OODA Loop 116
Defeating the Kill Chain 117
Operationalizing Risk Mitigation: Step by Step 118
Step 1: Assess the Existing Architectures 119
Step 2: Assess Vulnerabilities and Threats 126
Step 3: Select Risk Treatment and Controls 135
Step 4: Implement Controls 141
Step 5: Authorize: Senior Leader Acceptance and Ownership 146
The Ongoing Job of Keeping Your Baseline Secure 146
Build and Maintain User Engagement with Risk Controls 147
Participate in Security Assessments 148
Manage the Architectures: Asset Management and Configuration Control 151
Ongoing, Continuous Monitoring 152
Exploiting What Monitoring and Event Data Is Telling You 155
Incident Investigation, Analysis, and Reporting 159
Reporting to and Engaging with Management 160
Summary 161
Exam Essentials 161
Review Questions 166

Part III The Technologies of Information Security 173

Chapter 5 Communications and Network Security 175

Trusting Our Communications in a Converged World 176
Introducing CIANA 179
Threat Modeling for Communications Systems 180
Internet Systems Concepts 181
Datagrams and Protocol Data Units 182
Handshakes 184
Packets and Encapsulation 185
Addressing, Routing, and Switching 187
Network Segmentation 188
URLs and the Web 188
Topologies 189
"Best Effort" and Trusting Designs 193

Two Protocol Stacks, One Internet 194
Complementary, Not Competing, Frameworks 194
Layer 1: The Physical Layer 198
Layer 2: The Data Link Layer 199
Layer 3: The Network Layer 201
Layer 4: The Transport Layer 202
Layer 5: The Session Layer 206
Layer 6: The Presentation Layer 207
Layer 7: The Application Layer 208
Cross-Layer Protocols and Services 209
IP and Security 210
Layers or Planes? 211
Software-Defined Networks 212
Virtual Private Networks 213
A Few Words about Wireless 214
IP Addresses, DHCP, and Subnets 217
IPv4 Address Classes 217
Subnetting in IPv4 219
IPv4 vs. IPv6: Key Differences and Options 221
CIANA Layer by Layer 223
CIANA at Layer 1: Physical 223
CIANA at Layer 2: Data Link 226
CIANA at Layer 3: Network 228
CIANA at Layer 4: Transport 229
CIANA at Layer 5: Session 230
CIANA at Layer 6: Presentation 231
CIANA at Layer 7: Application 232
Securing Networks as Systems 233
A SOC Is Not a NOC 234
Tools for the SOC and the NOC 235
Integrating Network and Security Management 236
Summary 238
Exam Essentials 238
Review Questions 243

Chapter 6 Identity and Access Control 249

Identity and Access: Two Sides of the Same CIANA Coin 250
Identity Management Concepts 251
Identity Provisioning and Management 252
Identity and AAA 254
Access Control Concepts 255
Subjects and Objects—Everywhere! 257
Data Classification and Access Control 258

Bell-LaPadula and Biba Models 260
Role-Based 263
Attribute-Based 263
Subject-Based 264
Object-Based 264
Mandatory vs. Discretionary Access Control 264
Network Access Control 265
IEEE 802.1X Concepts 267
RADIUS Authentication 268
TACACS and TACACS+ 269
Implementing and Scaling IAM 270
Choices for Access Control Implementations 271
"Built-in" Solutions? 273
Multifactor Authentication 274
Server-Based IAM 276
Integrated IAM systems 277
Zero Trust Architectures 281
Summary 282
Exam Essentials 283
Review Questions 290

Chapter 7 Cryptography 297

Cryptography: What and Why 298
Codes and Ciphers: Defining Our Terms 300
Cryptography, Cryptology, or…? 305
Building Blocks of Digital Cryptographic Systems 306
Cryptographic Algorithms 307
Cryptographic Keys 308
Hashing as One-Way Cryptography 310
A Race Against Time 313
"The Enemy Knows Your System" 314
Keys and Key Management 314
Key Storage and Protection 315
Key Revocation and Zeroization 315
Modern Cryptography: Beyond the "Secret Decoder Ring" 317
Symmetric Key Cryptography 317
Asymmetric Key (or Public Key) Cryptography 318
Hybrid Cryptosystems 318
Design and Use of Cryptosystems 319
Cryptanalysis (White Hat and Black Hat) 319
Cryptographic Primitives 320
Cryptographic Engineering 320
"Why Isn't All of This Stuff Secret?" 320

Cryptography and CIANA 322
Confidentiality 322
Authentication 323
Integrity 323
Nonrepudiation 324
"But I Didn't Get That Email…" 324
Availability 325
Public Key Infrastructures 327
Diffie-Hellman-Merkle Public Key Exchange 328
RSA Encryption and Key Exchange 331
ElGamal Encryption 331
Digital Signatures 332
Digital Certificates and Certificate Authorities 332
Hierarchies (or Webs) of Trust 333
Pretty Good Privacy 337
TLS 338
HTTPS 340
Symmetric Key Algorithms and PKI 341
PKI and Trust: A Recap 342
Other Protocols: Applying Cryptography to Meet Different Needs 344
IPSec 344
S/MIME 345
DKIM 345
Blockchain 346
Access Control Protocols 348
Measures of Merit for Cryptographic Solutions 348
Attacks and Countermeasures 349
Brute Force and Dictionary Attacks 350
Side Channel Attacks 350
Numeric (Algorithm or Key) Attacks 351
Traffic Analysis, "Op Intel," and Social Engineering Attacks 352
Massively Parallel Systems Attacks 353
Supply Chain Vulnerabilities 354
The "Sprinkle a Little Crypto Dust on It" Fallacy 354
Countermeasures 355
On the Near Horizon 357
Pervasive and Homomorphic Encryption 358
Quantum Cryptography and Post–Quantum Cryptography 358
AI, Machine Learning, and Cryptography 360
Summary 361
Exam Essentials 361
Review Questions 366

Chapter 8 Hardware and Systems Security 371

Infrastructure Security Is Baseline Management 372
It's About Access Control… 373
It's Also About Supply Chain Security 374
Do Clouds Have Boundaries? 375
Infrastructures 101 and Threat Modeling 376
Hardware Vulnerabilities 379
Firmware Vulnerabilities 380
Operating Systems Vulnerabilities 382
Virtual Machines and Vulnerabilities 385
Network Operating Systems 386
MDM, COPE, and BYOD 388
BYOI? BYOC? 389
Malware: Exploiting the Infrastructure's Vulnerabilities 391
Countering the Malware Threat 394
Privacy and Secure Browsing 395
"The Sin of Aggregation" 397
Updating the Threat Model 398
Managing Your Systems' Security 399
Summary 399
Exam Essentials 400
Review Questions 407

Chapter 9 Applications, Data, and Cloud Security 413

It's a Data-Driven World…At the Endpoint 414
Software as Appliances 417
Applications Lifecycles and Security 420
The Software Development Lifecycle (SDLC) 421
Why Is (Most) Software So Insecure? 424
Hard to Design It Right, Easy to Fix It? 427
CIANA and Applications Software Requirements 428
Positive and Negative Models for Software Security 431
Is Blacklisting Dead? Or Dying? 432
Application Vulnerabilities 434
Vulnerabilities Across the Lifecycle 434
Human Failures and Frailties 436
"Shadow IT:" The Dilemma of the User as Builder 436
Data and Metadata as Procedural Knowledge 438
Information Quality and Information Assurance 440
Information Quality Lifecycle 441
Preventing (or Limiting) the "Garbage In" Problem 442

Protecting Data in Motion, in Use, and at Rest 443
Data Exfiltration I: The Traditional Threat 445
Detecting Unauthorized Data Acquisition 446
Preventing Data Loss 447
Into the Clouds: Endpoint App and Data Security Considerations 448
Cloud Deployment Models and Information Security 449
Cloud Service Models and Information Security 450
Clouds, Continuity, and Resiliency 452
Clouds and Threat Modeling 453
Cloud Security Methods 455
SLAs, TORs, and Penetration Testing 456
Data Exfiltration II: Hiding in the Clouds 456
Legal and Regulatory Issues 456
Countermeasures: Keeping Your Apps and Data Safe and Secure 458
Summary 459
Exam Essentials 460
Review Questions 470

Part IV People Power: What Makes or Breaks Information Security 477

Chapter 10 Incident Response and Recovery 479

Defeating the Kill Chain One Skirmish at a Time 480
Kill Chains: Reviewing the Basics 482
Events vs. Incidents 484
Incident Response Framework 485
Incident Response Team: Roles and Structures 487
Incident Response Priorities 490
Preparation 491
Preparation Planning 491
Put the Preparation Plan in Motion 493
Are You Prepared? 494
Detection and Analysis 497
Warning Signs 497
Initial Detection 499
Timeline Analysis 500
Notification 500
Prioritization 501
Containment and Eradication 502
Evidence Gathering, Preservation, and Use 504
Constant Monitoring 505

Recovery: Getting Back to Business 505
Data Recovery 506
Post-Recovery: Notification and Monitoring 508
Post-Incident Activities 508
Learning the Lessons 509
Support Ongoing Forensics Investigations 510
Information and Evidence Retention 511
Information Sharing with the Larger IT Security Community 511
Summary 512
Exam Essentials 512
Review Questions 518

Chapter 11 Business Continuity via Information Security and People Power 525

A Spectrum of Disruption 526
Surviving to Operate: Plan for It! 529
Cloud-Based "Do-Over" Buttons for Continuity, Security, and Resilience 531
CIANA at Layer 8 and Above 537
It *Is* a Dangerous World Out There 539
People Power for Secure Communications 541
POTS and VoIP Security 542
Summary 543
Exam Essentials 544
Review Questions 547

Chapter 12 Risks, Issues, and Opportunities, Starting Tomorrow 553

On Our Way to the Future 554
Access Control and Zero Trust 555
AI, ML, BI, and Trustworthiness 556
Quantum Communications, Computing, and Cryptography 557
Paradigm Shifts in Information Security? 558
Perception Management and Information Security 559
Widespread Lack of Useful Understanding of Core Technologies 560
IT Supply Chain Vulnerabilities 561
Government Overreactions 561
CIA, CIANA, or CIANAPS? 562

Enduring Lessons 563
You Cannot Legislate Security 563
It's About Managing Our Security and Our Systems 563
People Put It Together 564
Maintain Flexibility of Vision 565
Accountability—It's Personal. Make It So. 565
Stay Sharp 566
Your Next Steps 567
At the Close 568

Appendix Answers to Review Questions 569

Self-Assessment 570
Chapter 2: Information Security Fundamentals 576
Chapter 3: Integrated Information Risk Management 579
Chapter 4: Operationalizing Risk Mitigation 581
Chapter 5: Communications and Network Security 583
Chapter 6: Identity and Access Control 586
Chapter 7: Cryptography 589
Chapter 8: Hardware and Systems Security 592
Chapter 9: Applications, Data, and Cloud Security 594
Chapter 10: Incident Response and Recovery 597
Chapter 11: Business Continuity via Information Security and People Power 601

Index *605*

Foreword

Welcome to the *(ISC)² SSCP Systems Security Certified Practitioner Official Study Guide, Second Edition*! The global cybersecurity talent gap represents a huge opportunity for you to leverage your information technology skills to help protect your organization's infrastructure, information, systems, and processes and to improve and grow in your professional journey.

The Systems Security Certified Practitioner is a foundational certification that demonstrates you have the advanced technical skills and knowledge to implement, monitor, and administer IT infrastructure using security best practices, policies, and procedures established by the cybersecurity experts at (ISC)² for protecting critical assets. This book will guide you through the seven subject area domains on which the SSCP exam will test your knowledge. Step by step, it will cover the fundamentals involved in each topic and will gradually build toward more focused areas of learning in order to prepare you.

The SSCP is a mark of distinction that hiring managers look for when recruiting for roles that include cybersecurity responsibilities. Your pursuit and maintenance of this credential demonstrates that you have the knowledge and the drive to meet a recognized standard of excellence.

Whether you are brand new to the field or just want a refresher on the core tenets of cybersecurity, this guide will help you build a solid understanding of the technical, physical, administrative and legal aspects of the information security and assurance profession, as well as the ethical fidelity required of the SSCP.

I hope that you will find the *(ISC)² SSCP Systems Security Certified Practitioner Official Study Guide, Second Edition* to be an informative and helpful tool and wish you great success in your preparation and your professional growth.

Sincerely,

David P. Shearer, CISSP
CEO, (ISC)²

Introduction

Congratulations on choosing to become a Systems Security Certified Practitioner (SSCP)! In making this choice, you're signing up to join the "white hats," the professionals who strive to keep our information-based modern world safe, secure, and reliable. SSCPs and other information security professionals help businesses and organizations keep private data *private* and help to ensure that published and public-facing information stays unchanged and unhacked.

Whether you are new to the fields of information security, information assurance, or cybersecurity, or you've been working with these concepts, tools, and ideas for some time now, this book is here to help you grow your knowledge, skills, and abilities as a systems security professional.

Let's see how!

About This Book

You're here because you want to learn what it takes to be an SSCP. You know this will demand that you build a solid understanding of many different concepts, not only as theories but also as practical tasks you can *do* to help make information systems more secure. You know you'll need to master a number of key definitions and be able to apply those definitions to real-world situations—you'll need to operationalize those definitions and concepts by turning them into the step-by-step operations that *make* security become real.

This book is your study guide. It guides you along your personal journey as you learn and master these ideas and technologies. It takes you on that journey concept by concept, starting with simple, fundamental ideas and growing them to the level of power and complexity *you* will need, on the job, as an SSCP. That is this book's focus, its purpose, and design.

In doing so, it's also a valuable reference to have with you on the job, or as you continue to learn more about information security, information risk management, or any of a number of other related subject areas. You'll find it more than covers the topic domains that $(ISC)^2$ requires you to demonstrate competency in, should you wish to earn their Systems Security Certified Practitioner credential.

What Makes This the "Official" Study Guide for the SSCP?

Good question! This book exists because $(ISC)^2$ wanted a book that would teach as well as guide, explain as well as capture the common knowledge about keeping information systems secure, protecting information assets, and information assurance that all SSCPs should have at their mental fingertips. As creators of the SSCP program, $(ISC)^2$ defines that common body of knowledge, in continuous consultation with system security experts and practitioners from business, industry, government, and academia from around the world.

Using this official study guide, individuals can prepare for the SSCP exam with confidence. Businesses and other organizations can build their own in-house staff development and training programs around this book and have the same confidence that what they'll be training their people on aligns with $(ISC)^2$'s structure and definition of the SSCP as a body of knowledge.

What Is an SSCP?

The SSCP is actually three things in one: a standard of excellence, a credential that attests to demonstrated excellence, and a *person* who has earned that credential. Perhaps instead of asking "what" is an SSCP, we should also ask *why, who,* and *how*:

- *SSCP as standard of excellence*. The International Information System Security Certification Consortium, or $(ISC)^2$, created this standard to reflect the continually evolving needs for people who can help all sorts of organizations around the world keep their information systems safe, secure, confidential, private, reliable, and trustworthy. Working with businesses, nonprofits, academic researchers, and the thought leaders of the cybersecurity and information assurance communities of practice, they developed the list of subject areas, or *domains*, that are the SSCP as a standard. That standard is set as the starting point for your professional journey as an information security specialist. Its focus is on hands-on technical knowledge combined with procedural and administrative awareness. The knowledge, skills, and abilities that make up the SSCP domains become the foundation for other, more advanced certifications (and hence standards).
- *SSCP as a credential*. Earning an SSCP certification attests to the fact that you have solid working knowledge of the topic domains that are the SSCP. As a published standard of excellence, this certification or credential is portable—people in the information system business, or who know the needs of their own organizations for information security, recognize and respect this credential. People can easily consult $(ISC)^2$'s published standards for the SSCP and understand what it means. It is a portable, stackable credential, meaning that it can clearly pave the way for you to take on job responsibilities that need the knowledge and skills it attests to, and demonstrates you have the foundational knowledge to earn other credentials that can build on it.
- *SSCP as a goal or objective*. The SSCP as a standard answers the needs of hiring managers when they seek the right kind of people to help protect their organization's information, their information systems and processes, their IT infrastructure, and their ability to make informed decisions in reliable, timely ways. Training managers or functional department leaders in various organizations can design their own internal training and skills development programs around the SSCP, knowing that it is a reliable standard for information system security knowledge and experience. They can look at job descriptions or task designs, and use the SSCP as a standard to identify whether the job and the SSCP are a good fit with each other, or if other significant knowledge and skills will be needed by people filling that position.
- *SSCP as a person*. By choosing to earn an SSCP credential, you're declaring to yourself and to others that you're willing to hold yourself to a respected and recognized standard of excellence. You're willing to master what that standard asks of you, not only on the technical, physical, and administrative aspects of information security and assurance, but also on its legal and ethical requirements.

The *Systems Security Certified Practitioner* is thus a person who does the job of systems security to a level of competency that meets or exceeds that standard and who has earned a credential as testament to their knowledge and skills. It is a foundational certification, based on the knowledge and skills that people should already have when they first start out as an information security professional.

Let's *operationalize* that set of words by showing them in action:

- *Systems*—Generally, a *system* is a collection or set of elements that interconnect and interact with each other to fulfill or achieve a larger purpose or objective. In this context, we mean *information systems*. *Information systems* are the collected sets of hardware, software, databases, and data sets; the communications, networking, and other technologies that connect all of those elements together into a cohesive, working whole; and the people who use them and depend on them to achieve their goals and objectives.
- *Security*—Again, generally speaking, security is the set of plans, procedures, and actions that keep something safe from harm, damage, or loss, through accident, acts of nature, or deliberate actions taken by people. Applying that to information systems, we see that *information systems security* is everything we need to do during design, implementation, operational use, and maintenance to keep all aspects of an information system protected against accidental or deliberate damage; it includes keeping its information free from unauthorized changes or viewing; and it keeps those systems up and running so that the information is there when people need it to get their jobs done.
- *Certified*—The person holding this credential (or certification) has earned the right to do so by means of having demonstrated their mastery of the knowledge, skills, and attitudes that are defined to be the subject area or domain of the certification. Specifically, an SSCP has passed the certification exam and demonstrated the required work experience in the field of information security, as specified by the SSCP subject area domains.
- *Practitioner*—A person whose professional or workplace duties, responsibilities, and tasks has them using the knowledge, skills, and abilities required by the standard to have earned the certification. There's a degree of *practice* in the definition of *practitioner*, of course; as a practitioner, you are continually *doing* the stuff of your profession, and in doing so you continue to *learn it better* as well as refine, polish, and enrich the ways in which you do those tasks and fulfill those responsibilities. Practitioners get better with practice! (After all, if you've been "practicing medicine" for 20 years, we expect you are a much better medical doctor now than you were when you started.)

Note that a practitioner may be a specialist or a generalist; this is usually defined by the standards issued by the credentialing organization and reflects accepted and valued practice in the profession or industry as a whole.

What Can We Expect of Our SSCPs?

The world of commerce, industry, and governance expects you, as an SSCP, to be a hands-on practitioner of information systems security, someone who continuously monitors information systems to safeguard against security threats, vulnerabilities, and risks while having the knowledge to apply security concepts, tools, and procedures to react to security incidents. As an SSCP, you demonstrate certain knowledge and skills, in areas such as:

- Information technology and cybersecurity theory and hands-on/technical practice
- Cybersecurity policy, procedures, standards, and guidelines
- Using simple coding or programming language techniques, in languages such as command line interface, PowerShell, Java, HTML, CSS, Python, and C#

You'll also need more than just technical skills and knowledge. As an SSCP, you'll be working with people constantly, as you assist them in securing their organization's information security needs. This takes adaptability on your part, plus strong interpersonal skills. You'll need to be a critical thinker, and to make sounds judgments; you'll have to communicate in person and in writing as you build and manage professional relationships within your organization and the larger information security community of practice. You'll build this social capital both through your problem-solving skills and by applying your emotional intelligence.

Soft Skills: Very Strong Tickets to Success

Employers, clients, and others you'll work with value your technical knowledge and skills, but they desperately need to be able to work with and communicate with you as you bring that knowledge and skills to bear on their problems. The irony of calling these skills "soft" is that for some of us, it can be very hard work to improve on them. Investing in improving these skills will more than pay off for you in terms of salary and opportunities.

It's also natural to expect that as an SSCP, you will be continually learning about your craft. You'll keep current about the ways that threats evolve and stay informed about known vulnerabilities as they might be exploited against the systems under your care. You'll know how to apply analytical and research skills to dig deeper into what you're seeing in the way those systems are behaving, with an eye to identifying problems, recognizing that an information security incident might be under way, and responding to such incidents. This also means that you will periodically reflect on what you've been doing, how you've been doing it, and what you've been learning, and consider where improvement and growth are required to ensure continued effectiveness.

Who Should Take the SSCP Certification Exam?

The SSCP designation is designed for individuals who desire to learn hands-on, technical, cybersecurity fundamentals. While any individual who desires to practice cybersecurity can learn the material, there are certain requirements before sitting for the exam. SSCP candidates must have at least one year of cumulative work experience in one or more of the seven domains of the (ISC)^2 SSCP Common Body of Knowledge (CBK). A one-year prerequisite pathway will be granted for candidates who received an accredited university degree (bachelor's or master's) in a cybersecurity program. Candidates without the required experience can take and pass the SSCP exam to earn an Associate of (ISC)^2 designation and will have up to two years to gain the work experience needed for the SSCP.

Certificate vs. Certification vs. "Being Certified"

If you're new to formal certifications, these terms may seem interchangeable—but they are not!

A *certificate* is an official document or proof that displays or attests to your completion of a formal program, school, or training course. Earning a certificate may require passing a formal exam, hands-on practice, or just remaining in the course until the end. Certificate courses are designed to teach a skill and/or influence knowledge and understanding of a topic.

A *certification* goes several steps further than a certificate. Typically, certifications require a minimum period of professional experience, which may include supervision by someone who also holds that same certifications.

Certifications are established by professional organizations that serve a particular industry, and thus earning that certification means you've demonstrated what that industry needs. Certificates are defined and issued by the schools or training programs that teach them.

Typically, certifications have requirements for ongoing learning, experience, and skills development; certificates usually do not.

Finally, consider who awards you that credential. If it's the school or the training organization, it's a certificate. If it's that standards-setting body, it's a certification.

As a result, you are entitled—you have earned the right—to put the official, accepted designation of that certification after your name, when used as a part of your professional correspondence, marketing, or other communications. John Doe, SSCP, or Jayne Smith, MD, are ways that these individuals rightfully declare their earned certifications.

Academic programs increasingly offer sets of accredited university courses bundled as certificate programs; instead of completing 120 semester hours for a bachelor's degree, for example, a certificate program might only require 15 to 30 semester hours of study.

Thus, we see that "being certified" means that you've met the standards required by the professional organization that defines and controls that certification as a process and as a standard; you've earned the right to declare yourself "certified" in the domain of that standard.

The National and International Need

We've certainly needed people who understood information security as a systems discipline since the dawn of the computer age, but it wasn't until the early 1990s that we saw national and global awareness of this need start to attract headlines and influence the ways people prepared for careers in cybersecurity. One of the results of the President's Commission on Critical Infrastructure Protection (PCCIP), created by Bill Clinton, was the recognition that the nation needed a far larger and more sustained effort focused on securing the Internet-based backbones and systems on which our society and much of the world depended upon for day-to-day business, commerce, public services, hygiene, transportation, medicine—in short, for everything! Virtually all of that infrastructure was owned and operated by private business; this was not something governments could mandate, direct, or perform.

The National Institute of Standards and Technology (NIST) took the lead in defining standards-based frameworks and approaches for identifying, managing, and controlling risks to information systems and infrastructures. As a part of this effort, NIST established the National Initiative for Cybersecurity Education (NICE). This partnership between government, academia, and the private sector works to continually define the standards and best practices that cybersecurity professional educators and trainers need to fulfill in order to produce a qualified cybersecurity workforce.

In the meantime, the Department of Defense (DoD) has continued its efforts to professionalize its workforce (both the uniformed and civilian members) and, in a series of regulations and directives, has defined its baseline set of approved certifications in various fields. One of these, DoD Directive 8140, defines the minimum acceptable certifications someone must demonstrate to hold jobs in the information assurance technical, managerial, and systems architecture job series. DoD 8140 also defines the certifications necessary to hold jobs as a cybersecurity service provider at various levels.

Internationally, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have jointly issued their own family of standards designed to help private and public organizations worldwide attain minimum acceptable standards in achieving information security, information assurance, and cybersecurity. The ISO/IEC 27000 family of standards provides best practice recommendations on information security management and the management of information risks through information security controls, within the context of an overall information security management system (ISMS). ISO/IEC 27001 is the best-known standard in the family providing requirements for an ISMS. The European Union has issued a series of regulations and policy documents that help refine and implement these ISO/IEC standards.

$(ISC)^2$ plays a part in helping all of these standards bodies and regulatory agencies assess the current needs of the information security community of practitioners and works to update its set of certifications to support these national, international, and global needs. As a result, the SSCP certification is recognized around the world.

The SSCP and Your Professional Growth Path

Possibly one of the best ways to see your SSCP in the context of your professional growth and development can be seen at the CyberSeek website. CyberSeek is a partnership sponsored by NIST that brings together the current state of the job market in cybersecurity, information security, and information risk management. It combines data on job market demand for such skills, current average salaries, and even insight on the numbers of professionals holding various certifications. The real gem, however, for the new cybersecurity or information security pro is its Career Mapping tool. See this at `www.cyberseek.org` and use it to help navigate the options to consider and the opportunities that an earned SSCP after your name might open up.

As an international, nonprofit membership association with more than 140,000 members, (ISC)² has worked since its inception in 1989 to serve the needs for standardization and certification in cybersecurity workplaces around the world. Since then, (ISC)²'s founders and members have been shaping the information security profession and have developed the following information security certifications:

- Certified Information Systems Security Professional (CISSP): The CISSP is an experienced professional who holds the most globally recognized standard of achievement in the industry, and the first information security credential to meet the strict conditions of ISO/IEC Standard 17024. The CISSP certification has three concentrations:
  - Certified Information Systems Security Professional: Information Systems Security Architecture Professional (CISSP-ISSAP): The CISSP-ISSAP is a chief security architect, analyst, or other professional who designs, builds, and oversees the implementation of network and computer security for an organization. The CISSP-ISSAP may work as an independent consultant or other professional who provides operational guidance and direction to support business strategies.
  - Certified Information Systems Security Professional: Information Systems Security Engineering Professional (CISSP-ISSEP): The CISSP-ISSEP can effectively incorporate security into all facets of business operations.
  - Certified Information Systems Security Professional: Information Systems Security Management Professional (CISSP-ISSMP): The CISSP-ISSMP is a cybersecurity manager who demonstrates deep management and leadership skills and excels at establishing, presenting, and governing information security programs.
- Systems Security Certified Practitioner (SSCP): The SSCP is a high-value practitioner who demonstrates technical skills in implementing, monitoring, and administering IT infrastructure using information security policies and procedures. The SSCP's commitment to continuous learning and practice ensures consistent information assurance.
- Certified Cloud Security Professional (CCSP): The CCSP is a globally recognized professional who demonstrates expertise and implements the highest standards in cloud security. The certification was co-created by (ISC)² and Cloud Security Alliance—the leading stewards for information security and cloud computing security.

- Certified Authorization Professional (CAP): The CAP is a leader in information security and aligns information systems with the risk management framework (RMF). The CAP certification covers the RMF at an extensive level, and it's the only certification under the DoD 8570/DoD 8140 Approved Baseline Certifications that aligns to each of the RMF steps.
- Certified Secure Software Lifecycle Professional (CSSLP): The CSSLP is an internationally recognized professional with the ability to incorporate security practices—authentication, authorization, and auditing—into each phase of the software development lifecycle (SDLC).
- HealthCare Information Security and Privacy Practitioner (HCISPP): The HCISSP is a skilled practitioner who combines information security with healthcare security and privacy best practices and techniques.

Each of these certifications has its own requirements for documented full-time experience in its requisite topic areas.

Newcomers to information security who have not yet had supervised work experience in the topic areas can take and pass the SSCP exam and then become recognized as Associates of $(ISC)^2$. Associates then have two years to attain the required experience to become full members of $(ISC)^2$.

The SSCP Seven Domains

$(ISC)^2$ is committed to helping members learn, grow, and thrive. The Common Body of Knowledge (CBK) is the comprehensive framework that helps it fulfill this commitment. The CBK includes all the relevant subjects a security professional should be familiar with, including skills, techniques, and best practices. $(ISC)^2$ uses the various domains of the CBK to test a certificate candidate's levels of expertise in the most critical aspects of information security. You can see this framework in the SSCP Exam Outline at `www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/SSCP-Exam-Outline-Nov-1-2018.ashx`.

Successful candidates are competent in the following seven domains:

Domain 1: Access Controls Policies, standards, and procedures that define who users are, what they can do, which resources and information they can access, and what operations they can perform on a system, such as:

1.1 Implement and maintain authentication methods

1.2 Support internetwork trust architectures

1.3 Participate in the identity management lifecycle

1.4 Implement access controls

Domain 2: Security Operations and Administration Identification of information assets and documentation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability, such as:

2.1 Comply with codes of ethics

2.2 Understand security concepts

2.3 Document, implement, and maintain functional security controls

2.4 Participate in asset management

2.5 Implement security controls and assess compliance

2.6 Participate in change management

2.7 Participate in security awareness and training

2.8 Participate in physical security operations (e.g., data center assessment, badging)

Domain 3: Risk Identification, Monitoring, and Analysis Risk identification is the review, analysis, and implementation of processes essential to the identification, measurement, and control of loss associated with unplanned adverse events. Monitoring and analysis are determining system implementation and access in accordance with defined IT criteria. This involves collecting information for identification of, and response to, security breaches or events, such as:

3.1 Understand the risk management process

3.2 Perform security assessment activities

3.3 Operate and maintain monitoring systems (e.g., continuous monitoring)

3.4 Analyze monitoring results

Domain 4: Incident Response and Recovery "The show must go on" is a well-known saying that means even if there are problems or difficulties, an event or activity must continue. Incident response and recovery ensures the work of the organization will continue. In this domain, the SSCP gains an understanding of how to handle incidents using consistent, applied approaches like business continuity planning (BCP) and disaster recovery planning (DRP). These approaches are utilized to mitigate damages, recover business operations, and avoid critical business interruption:

4.1 Support incident lifecycle

4.2 Understand and support forensic investigations

4.3 Understand and support business continuity plan (BCP) and disaster recovery plan (DRP) activities

Domain 5: Cryptography The protection of information using techniques that ensure its integrity, confidentiality, authenticity, and nonrepudiation, and the recovery of encrypted information in its original form:

5.1 Understand fundamental concepts of cryptography

5.2 Understand reasons and requirements for cryptography

5.2 Understand and support secure protocols

5.2 Understand public key infrastructure (PKI) systems

Domain 6: Network and Communications Security The network structure, transmission methods and techniques, transport formats, and security measures used to operate both private and public communication networks:

6.1 Understand and apply fundamental concepts of networking

6.2 Understand network attacks and countermeasures (e.g., DDoS, man-in-the-middle, DNS poisoning)

6.3 Manage network access controls

6.4 Manage network security

6.5 Operate and configure network-based security devices

6.6 Operate and configure wireless technologies (e.g., Bluetooth, NFC, Wi-Fi)

Domain 7: Systems and Application Security Countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses, and other related forms of intentionally created damaging code:

7.1 Identify and analyze malicious code and activity

7.2 Implement and operate endpoint device security

7.3 Operate and configure cloud security

7.4 Operate and secure virtual environments

Using This Book

This book is structured to take you on your learning journey through all seven subject area domains that the SSCP requires. It does this one building block at a time, starting with the fundamentals involved in a particular topic or subject, and building on those to guide you toward the degree of knowledge you'll need as an SSCP. This book is structured in four major parts:

- Part 1 provides a solid foundation of how organizations use information to drive decision making, and the role of information systems and information technologies in making that information available, reliable, and useful. It then looks to the fundamental concepts of information security and assurance, using operational definitions and examples to help you apply these concepts to real-world situations you may find around you today:
  - Business and the private sector speak their own language, and organize, direct, manage, and lead their people in different ways than do governments or military services. If you haven't had experience in the private sector or have no business background, start with Chapter 1.

Using the Language of Business

Chapter 1's content is valuable to every SSCP, but it is not officially a part of the SSCP domains, and is outside the scope of the SSCP certification exam. Even if you've had private sector work experience, you'll find Chapter 1 will strengthen your understanding of *why* business finds information security and assurance so important. With that as foundation, you can go on and learn *how* to make that security happen.

  - Chapter 2 provides a deep look at the fundamentals of information security and assurance.

- Part 2 takes you deep into the practice of risk management, with great emphasis on information risk management:
  - Chapter 3 defines the basic concepts of risk management and risk mitigation and familiarizes you with the processes all organizations can use to understand risks, characterize their impact on organizational objectives, and prioritize how to deal with information risks specifically.
  - Chapter 4 dives into risk mitigation. Here's where we make decisions about specific risks (or, rather, about the vulnerabilities we've discovered that could lead to such a risk becoming reality). We'll look at choices you can make, or advise your company's management to make, and how you can estimate the value of your mitigation choices as compared to the possible impacts if nothing is done.
- Part 3 gets down into the technologies of information security; we'll start each major subject area in Part 3 first by reviewing the fundamentals of various information systems technologies and how they are used, and then look to their vulnerabilities and what choices we might have to help mitigate their associated risks. Key throughout Part 3 is the need to own and manage the baseline architectures of our information systems—for without effective management of our systems, we have little hope of being able to keep them secure, much less operating correctly!
  - Chapter 5 is all about communications as a people-to-people and systems-to-systems set of processes and *protocols*. Two *protocol stacks*—the Open Systems Interconnection (OSI) 7-layer reference model and the Transmission Control Protocol over Internet Protocol (TCP/IP)—will become your highway to understanding and appreciating the different perspectives you'll need as you seek to secure networks and systems.
  - Chapter 6 considers identity management and access control, which are two sides of the same process: how do we know that users or processes asking to use our systems and our information are who they claim they are, and how do we control, limit, or deny their access to or use of any of our information, our systems, our knowledge, or our people?
  - Chapter 7 demystifies cryptography and cryptographic systems, with special emphasis on the use of symmetric and asymmetric encryption algorithms as part of our digital certificates, signatures, and public infrastructure for security.
  - Chapter 8 considers the security aspects of computing and communications hardware, and the systems software, utilities, firmware, and connections that bring that all together.
  - Chapter 9 continues on the foundation laid in Chapter 8 by investigating how we secure applications software, data, and endpoint devices. It also looks at the specific issues involved when organizations migrate their information systems to the cloud (or have developed them in the cloud from the beginning).

- Part 4 shifts the emphasis back onto the real driving, integrative force that we need to apply to our information security problems: the people power inherent in our workforce, their managers and leaders, even our customers, clients, and those we partner with or share federated systems with:
  - Chapter 10 takes us through the information security incident response process, from planning and preparation through the real-time challenges of detection, identification, and response. It then takes us through the post-response tasks and shows how attention to these can increase our organization's chances of never having to cope with making the same mistakes twice by learning from the experiences of an incident response while they're still fresh in our response team members' minds.
  - Chapter 11 addresses business continuity and disaster recovery, which are both the overriding purpose of information security and assurance and the worst-case scenario for why we need to plan and prepare if we want our organization to survive a major incident and carry on with business as usual.
  - Chapter 12 takes a look back across all chapters and highlights important issues and trends which you as an SSCP may have to deal with in the very near future. It also offers some last-minute practical advice on getting ready to take your SSCP exam and ideas for what you can do after that.

As you look at the chapters and the domains, you should quickly see that some domains fit neatly into a chapter all by themselves; other domains share the limelight with each other in the particular chapters that address their subject areas. You'll also see that some chapters focus on building foundational knowledge and skills; others build applied problem-solving skills and approaches; and some provide a holistic, integrated treatment spanning CBK domains. This is intentional—the design of this book takes you on a journey of learning and mastery of those seven CBK domains.

Risk identification, monitoring, and analysis *as a domain* is a fundamental element of two chapters (Chapters 3 and 4) almost by itself. This important topic deserves this level of attention; you might even say that the very reason we *do* information security at all is because we're trying to manage and mitigate risks to our information! Similarly, we see that Chapter 11, which focuses on the people power aspects of achieving business continuity in the face of information security incidents and disasters, must make significant use of the *domains* of access control, security operations and administration, and risk identification, monitoring, and analysis. Finally, the growing emphasis in the marketplace on data security, cloud security, endpoint security, and software lifecycle security dictates that we first build a strong foundation on hardware and systems security (Chapter 8), on which we build our knowledge and skills for applications, data, cloud, and mobile endpoint security.

Objective Map

Table I.1 contains an objective map to show you at-a-glance where you can find each objective covered. Note that all chapters except Chapters 1 and 12 cover objectives from the SSCP exam.

TABLE I.1 Objective Map

Objective	Chapter
Domain 1: Access Controls	
1.1 Implement and maintain authentication methods	6
1.2 Support internetwork trust architectures	6
1.3 Participate in the identity management lifecycle	6, 11
1.4 Implement access controls	6
Domain 2: Security Operations and Administration	
2.1 Comply with codes of ethics	2, 11
2.2 Understand security concepts	2, 11
2.3 Document, implement, and maintain functional security controls	11
2.4 Participate in asset management	11
2.5 Implement security controls and assess compliance	3, 4
2.6 Participate in change management	3, 4
2.7 Participate in security awareness and training	3, 4, 11
2.8 Participate in physical security operations (e.g., data center assessment, badging)	3, 4

(continued)

TABLE I.1 Objective Map *(continued)*

Objective	Chapter
Domain 3: Risk Identification, Monitoring, and Analysis	
3.1 Understand the risk management process	3, 4
3.2 Perform security assessment activities	4
3.3 Operate and maintain monitoring systems (e.g., continuous monitoring)	4, 10
3.4 Analyze monitoring results	4
Domain 4: Incident Response and Recovery	
4.1 Support incident lifecycle	10
4.2 Understand and support forensic investigations	10
4.3 Understand and support business continuity plan (BCP) and disaster recovery plan (DRP) activities	10
Domain 5: Cryptography	
5.1 Understand fundamental concepts of cryptography	7
5.2 Understand reasons and requirements for cryptography	7
5.2 Understand and support secure protocols	7
5.2 Understand public key infrastructure (PKI) systems	7
Domain 6: Network and Communications Security	
6.1 Understand and apply fundamental concepts of networking	5
6.2 Understand network attacks and countermeasures (e.g., DDoS, man-in-the-middle, DNS poisoning)	5
6.3 Manage network access controls	6
6.4 Manage network security	5
6.5 Operate and configure network-based security devices	5
6.6 Operate and configure wireless technologies (e.g., Bluetooth, NFC, Wi-Fi)	5

Objective	Chapter
Domain 7: Systems and Application Security	
7.1 Identify and analyze malicious code and activity	8
7.2 Implement and operate endpoint device security	8, 9
7.3 Operate and configure cloud security	8, 9
7.4 Operate and secure virtual environments	8, 9

Earning Your Certification

Earning your SSCP requires that you take and pass the SSCP exam, of course; it also requires that you have at least one year of full-time work experience, in at least one of the seven domains of knowledge of the SSCP. A one-year prerequisite waiver will be granted by $(ISC)^2$ if you have earned a bachelor's degree or higher in a recognized cybersecurity-related discipline. The website `www.isc2.org/Certifications/SSCP/Prerequisite-Pathway` explains this and should be your guide. Note the requirements to be able to document your work experience.

No matter where you are on that pathway right now, put this book to work! Use it as a ready reference, as a roadmap, and as a learning tool. Let it help you broaden and deepen your knowledge base, while you sharpen your skills on the job or in your classes—or both!

Before the Exam: Grow Your Knowledge, Skills, and Experience

The key to this or any personal and professional development you wish to achieve is to first set your goals. SMART goals can help you plan and achieve most anything you set your body, mind, heart and spirit to:

- *Specific*—What is it, *exactly,* that you want to achieve?
- *Measurable*—How will you know that you've achieved that specific goal?
- *Achievable*—Is it really within your power and ability to achieve it? Or do you need to first build other strengths, develop other talents, or align other resources to help you take this goal on?
- *Realistic*—Can you actually do this? Are there practical ways to go about accomplishing this goal?
- *Timely*—When, *exactly,* do you want or need to accomplish this goal by?

Having set SMART goals, set a plan; lay out the tasks you'll need to accomplish, and break those down, week by week, perhaps even day by day, to get to the goals of taking and passing the exam, and having the prerequisite experience or earned degree.

Start by thoroughly reading, and rereading, this study guide. Work through its review questions, not only to focus on why the *right* answers are in fact correct, but to identify and understand what's wrong with the *wrong* answers. Work through the case studies, and let them suggest other real-world issues to you as you do.

Other options to consider include:

- Volunteer, at work, school, or in your local community, to work with others on information security–related projects or tasks.
- Find a study buddy.
- Enlist the help and guidance of a mentor.
- Enroll in formal training courses for the SSCP, either face-to-face, virtual live online, or in other modes that suit you.
- Take college courses that prepare you for the SSCP or that help you master some or all of its domains of knowledge.
- Use other learning resources, such as videos, and IT and security blog sites.

If you're already working (even part-time) in an IT-related job, consider talking with your supervisor about your ambition to earn your SSCP; you might find a wealth of practical advice and assistance, right there at work!

The SSCP Exam

The SSCP exam is a computer-based examination, which you must take at an $(ISC)^2$ approved testing facility. Pearson VUE is $(ISC)^2$'s official and exclusive global testing partner, but be advised: not all Pearson VUE testing locations meet the special test security requirements that $(ISC)^2$ imposes on test-takers and proctors alike. Start by reviewing the testing terms and conditions here: `www.isc2.org/Register-for-Exam`.

Register early at `https://home.pearsonvue.com/isc2`, and select the SSCP as the certification exam you're pursuing. Check the availability of testing centers at or near locations that best suit your needs. Note that different testing centers have different schedule options, with some being more available on the weekends while others might be closed.

You don't have to pay at this step—you pay for your exam when you're ready to schedule the exam (and you're ready to schedule the exam once you know when you'll be ready to take and pass it!).

A great way to learn more about the exam process is to take a "test drive," using the exam demo and tutorial about the exam experience. You can find this on the Pearson VUE website, `www.pearsonvue.com/athena/athena.asp`.

Armed with driving or public transport directions and a map, find your way from home (or where you'll be coming to the test from) to the testing site of your choice. Check out how long that trip takes at the time of day you want to take the test—or at the times of day that center has a testing slot available! (Take this "test drive" a few days in advance.)

Plan ahead. Know how to get to the testing center an hour early. Be prepared!

(ISC)² Terms and Conditions

(ISC)² requires that all candidates for certification read and accept the terms and conditions here: `www.isc2.org/uploadedFiles/Certification_Programs/CBT-Examination-Agreement.pdf`. Candidates who do not agree to the terms and conditions will not be permitted to sit for any (ISC)² examination.

Nondisclosure Agreement (NDA)

You will be required to agree to the NDA that will be presented at the beginning of your exam. Failure to read/accept the agreement within the allotted 5 minutes will result in your exam ending and a forfeit of your exam fees. Please take a moment to review the agreement now so that you are familiar with it when you sit for your exam.

Exam Fees and Payment

An exam voucher may be attained in fees paid during the scheduling process on the Pearson VUE website: `https://home.pearsonvue.com/`. Vouchers may be obtained in bulk on the (ISC)² website. This is ideal for companies that are scheduling several people for various exams. The more vouchers purchased, the greater the discount.

Reschedule Policy

If you wish to reschedule your exam, you must contact Pearson VUE by phone, at least 24 hours prior to your exam appointment; if you contact them online, you must do this at least 48 hours ahead of your appointment. Rescheduling an exam less than 24 hours prior is subject to a same-day forfeit exam fee. Exam fees are also forfeited for no-shows. There is a $50 fee for exam reschedules.

Cancellation Policy

If you wish to cancel your exam, you must contact Pearson VUE 24 hours prior to your scheduled appointment. Canceling an exam less than 24 hours prior to your appointment or missing your exam may result in forfeiting your exam fees. There is a $100 fee for cancellations.

The Exam Structure and Format

During the SSCP exam, you will focus on recalling, recognizing, and indicating your understanding of the information and ideas presented in this study guide. The SSCP exam is *proctored*, which means you will be supervised by a neutral person (a proctor) at all times while taking the test. The exam is pass/fail.

There are 125 multiple-choice questions on the exam. Of that number, only 100 are graded, whereas the remaining 25 are evaluated by exam developers and used to inform future exams. You will not know which of the 100 questions will be graded, so be sure to answer all exam questions to the best of your ability. The questions are written to check that you remember, understand, and can apply what you've learned in the seven knowledge domains that make up the SSCP, and they are covered by this study guide. Here are some thoughts to keep in mind about these questions and the exam process itself:

- Each multiple-choice question will list four possible answers.
- There are no true or false questions.
- Expect scenario-based questions that describe a situation, then ask that you use the situation to select the correct multiple-choice answer.
- All acronyms are spelled out, such as the confidentiality, integrity, and availability (CIA) triad.
- Many questions will ask for the *most* or *least* correct answer.
- Some questions will contain logical operators, such as not, always, test, true, or false.

You are not penalized for wrong answers, so be sure to answer every question. You will need a score of 700 out of 1000 points to pass the exam. The questions are weighted. This means you may be required to have more or fewer than 70 questions answered correctly to pass the exam.

One of the benefits to candidates taking an examination via CBT is that most candidates receive their scores immediately upon completing their examination. In some cases, however, to ensure it is providing accurate and valid test results to candidates, (ISC)² must conduct periodic psychometric analyses of a group of candidates' responses before it releases their exam results. For the small number of candidates affected by this process, the candidates will receive their results within four to six weeks after taking the exam. (ISC)² apologizes in advance for this inconvenience to those candidates who will not receive their pass/fail status at the test centers, but this is an important part of (ISC)²'s quality assurance process to protect the integrity of the credentials. Candidates who are impacted by this process will be informed when they complete their tests.

Reasonable Accommodations

If you require reasonable and appropriate accommodations for exams, you can request special accommodations through (ISC)². Once these are approved, be sure to coordinate with your chosen test center to ensure that they can meet your needs. *Work through this process early.* The on-site test administrator will not have the power to grant you an accommodation at the time of your exam if it has not been approved in advance.

(ISC)² provides reasonable and appropriate accommodations for its exams for people who have demonstrated a need for test accommodations. If you wish to request an accommodation, please visit www.isc2.org/Register-for-Exam and click Requesting Special Accommodations for information on requesting an accommodation.

Test accommodations are individualized and considered on a case-by-case basis. Once an accommodation is approved by (ISC)², they will send it to Pearson VUE Accommodations. Please allow two to three business days for Pearson VUE to get this information. Then, call Pearson VUE at 800-466-0450 so that you can schedule your exam. Please don't start by scheduling through Pearson VUE's website or through their main registration phone line. Contact (ISC)² first.

Please note that the purpose of test accommodations is to provide examinees with full access to the test. However, they are not a guarantee of improved performance or test completion.

On the Day of the Exam

Plan to arrive at your test center at least 30 minutes before your exam start time. To check in, you'll need to

- Show two valid, unexpired forms of personal ID (examples include government-issued IDs such as a driver's license, passport, etc.). Both must have your signature, and one of the two must have your photo. For more information about acceptable IDs, please visit: www.isc2.org/Register-for-Exam, and click What You Need to Bring to the Test Center for more information.
- Provide your signature.
- Submit to a palm vein scan (unless it's prohibited by law).
- Have your photo taken. Hats, scarves, and coats may not be worn for your photo. You also can't wear these items in the test room.
- Leave your personal belongings outside the testing room. You'll have access to secure storage. Storage space is small, so plan ahead. Pearson VUE test centers do not assume responsibility for your personal belongings.

The test administrator (TA) will give you a short orientation. If you have already arranged for special accommodations for your testing, and (ISC)² and Pearson VUE have approved these, be sure to go over them with the TA. Then, the TA will escort you to a computer terminal. Upon concluding the exam, click the Finish or Submit button.

After the Exam

The proctor will escort you out of the room. You'll receive a printed copy of your preliminary examination report by the front desk attendant. The report will congratulate you for passing the exam, or, should you fail, list the domains you need to study again from weakest to strongest.

Upon successfully passing the SSCP exam, you are not yet certified until (ISC)² approves it. You must be endorsed by another (ISC)²-certified professional before the credential can be awarded. The New Endorsement Application is located here: `https://apps.isc2.org/Endorsement/#/Home`.

An endorser can be anyone who is an active (ISC)² credential holder and can attest to your assertions regarding professional experience and education (if applicable) and that you are in good standing within the cybersecurity industry.

If you do not know an (ISC)²-certified professional, you may request (ISC)² to endorse your application.

Although you can start and save a draft application, you must pass the exam for the selected certification before you can submit your application for endorsement.

If you do not yet possess the education and/or experience required for the certification, you can request to be an Associate of (ISC)², which requires only that you pass the credential exam.

Congratulations! You're Now an SSCP. Now What?

As a recognized member of a profession, you've voluntarily taken up the duties and obligations that come with that recognition. You also have gone through an open door to the opportunities and benefits that come with that status. Those benefits and obligations go hand in hand as you continue to grow and learn as an information systems security professional.

Maintaining the SSCP Certification

SSCP credentials are maintained in good standing by participating in various activities and gaining professional continuing professional education credits (CPEs). CPEs are obtained through numerous methods such as reading books, attending seminars, writing papers or articles, teaching classes, attending security conventions, and participating in many other qualifying activities. Visit the (ISC)^2 website for additional information concerning the definition of CPEs.

Individuals are required to post a minimum of 20 CPE credits each year on the (ISC)^2 member website. Generally, the CPE credit post will be recognized immediately by the system, but it's also subject to random audit. Please note that any CPEs accomplished prior to being awarded the (ISC)^2 certification may not be claimed. If an individual accomplishes more than 20 CPEs for one year, the remainder may be carried forward to the following year. The (ISC)^2 website describes CPEs as items gained external to your current employment duties.

Join a Local Chapter

As an SSCP, you've become one of over 23,000 (ISC)^2 members worldwide. They, like you, are there to share in the knowledge, experience, and opportunity to help accomplish the goals and objectives of being an information security professional. Many of these members participate in local area chapters, and (ISC)^2 has numerous local chapters around the world. You can find one in your area by visiting `www.isc2.org/Chapters`.

Being an active part of a local chapter helps you network with your peers as you share knowledge, exchange information about resources, and work on projects together. You can engage in leadership roles and participate in co-sponsored local events with other industry associations. You might write for or speak at (ISC)^2 events and help support other (ISC)^2 initiatives. You can also be a better part of your local community by participating in local chapter community service outreach projects.

Chapter membership earns you CPE credits and can make you eligible for special discounts on (ISC)^2 products and programs.

Let's Get Started!

This book is for you. This is your journey map, your road atlas, and your handbook. Make it work for you.

Choose your own course through it, based on what you already know, what the self-assessment tells you, and what you've experienced thus far in your work or studies.

Go for it.

Self-Assessment

1. Which statement about business continuity planning and information security is most correct?
   - **A.** Plans are useful only because they start the development of detailed procedures and processes, and thus, there is no need to maintain or improve such plans.
   - **B.** Planning is more important than the plans it produces.
   - **C.** Plans represent significant investments and decisions and thus should be updated only when significant changes to objectives or circumstances dictate.
   - **D.** Planning should continuously bring plans and procedures in tune with ongoing operational reality.

2. Which of the following statements about social engineering attacks is incorrect?
   - **A.** Most targeted individuals don't see the harm in responding or in answering simple questions posed by the attacker.
   - **B.** Most people believe they are too smart to fall for such obvious ploys, but they do anyway.
   - **C.** Most targeted individuals and organizations have effective tools and procedures to filter out phishing and related scams, so they are now better protected from such attacks.
   - **D.** Most people want to be trusting and helpful.

3. In general, what differentiates phishing from whaling attacks?
   - **A.** Phishing attacks tend to be used to gain access to systems via malware payloads or by getting recipients to disclose information, whereas whaling attacks try to get responsible managers to authorize payments to the attacker's accounts.
   - **B.** Phishing attacks are focused on businesses; whaling attacks are focused on high-worth individuals.
   - **C.** Whaling attacks tend to offer something that ought to sound "too good to be true," whereas phishing attacks masquerade as routine business activities such as package delivery confirmations.
   - **D.** Whaling attacks send out huge numbers of emails attempting to lure targeted individuals into responding or following a link; phishing attacks use telephones or other means of making personal contact with a selected target.

4. You're the only IT person at a small tool and die machine shop, which uses a LAN and cloud-hosted platforms to run the business on. The previous IT person had told your boss not to worry about the business being the target of a cyberattack. Which statement best lets you explain the real risks the company might face?
   - **A.** Since we don't handle consumer-level payment cards, and we really don't have any proprietary information, we probably don't have to worry about being a target.
   - **B.** We do share an extranet connection with key customers and suppliers, but it should prevent an attack on our systems that could lead to an attack on theirs.

C. Our cloud systems hosting company provides most of our security, and as long as we keep our systems on the factory floor and the workstations our staff use properly updated, we should be okay.

D. Since we haven't really done even a basic vulnerabilities assessment, we don't know what risks we could be facing. Let's do that much at least, and let that tell us what the next step should be. Soon.

5. Which of these steps would *not* help you limit or prevent attacks on your systems that attempt to spoof, corrupt, or tamper with data?

A. Ensure that firewalls, routers, and other network infrastructures filter for and block attempts to access network storage without authorization.

B. Develop and use an organizational data model and data dictionary that contain all data-focused business logic; use them to build and validate business processes and the apps that support them.

C. Implement data quality processes that ensure all data is fit for all purposes, in accordance with approved business logic.

D. Implement information classification, and use access control and identity management to enforce it.

6. Which of the following are not examples of "shadow IT" contributing to an information security problem? (Choose all that apply.)

A. One user defines a format or style sheet for specific types of documents for others in the division to use.

B. An end user writes special-purpose database queries and reports used to forecast sales and project production and inventory needs, which are reviewed and used at weekly division meetings.

C. Several users build scripts, flows, and other processing logic to implement a customer service help desk/trouble ticket system, using its own database on a shared use/collaboration platform that the company uses.

D. Users post documents, spreadsheets, and many other types of information on a company-provided shared storage system, making the information more freely available throughout the company.

7. Which statement about privacy and data protection is the most correct and most important?

A. International standards and agreements specify that personally identifiable information (PII) and information about an individual's healthcare, education, work, or credit history must be protected from unauthorized use or disclosure.

B. It's up to the organization that gathers, produces, uses, or disposes of such private data to determine what protection, if any, is needed.

C. Storing backup or archive copies of privacy-related information in a datacenter in another country, without doing any processing there, does not subject you to that country's data protection laws.

D. Sometimes, it seems cheaper to run the risk of fines or loss of business from a data breach involving privacy-related data than to implement proper data protection to prevent such a loss. While this might make financial sense, it is not legal or ethical to do so.

8. In which phase or phases of a typical data exfiltration attack would an attacker probably not make use of phishing? (Choose all that apply.)

- **A.** Reconnaissance and characterization
- **B.** Data gathering, clumping, masking, and aggregating
- **C.** Installing and using covert command and control capabilities
- **D.** Initial access

9. When choosing your countermeasures and tactics to protect hardware and systems software, you should start with which of the following?

- **A.** Published Current Vulnerabilities and Exposures (CVE) databases
- **B.** The information systems baseline that documents the systems your organization uses
- **C.** Your organization's business impact analysis
- **D.** Your organization's IT vulnerabilities assessment

10. What kind of malware attacks can corrupt or infect device-level firmware? (Choose all that apply.)

- **A.** SNMP-based attacks that can trigger the device to download and install a firmware update remotely
- **B.** Remote or onsite device management (or mismanagement) attacks that allow a hacker to initiate a firmware update using a hacked firmware file
- **C.** Phishing or misdirection attacks that fool operators or users into initiating an upload of a hacked firmware file
- **D.** None, because firmware updates require operator intervention to download trusted updates and patch files from the manufacturer's or vendor's websites, and then initiate and monitor the update and restart of the device

11. What is a zero day exploit?

- **A.** An exploit conducted against a vulnerability within the same day as it is reported
- **B.** An exploit that impacts a system immediately, rather than having a delayed effect like ransomware or scareware does
- **C.** There are no real zero day exploits, but the mass media has exaggerated the dangers of unreported vulnerabilities
- **D.** An exploit conducted against a newly discovered vulnerability before it becomes known to the cybersecurity community or the system's vendor or owners

12. Which of the following statements best summarizes the benefits of using trusted platform modules (TPMs) as part of an organization's IT infrastructure?

- **A.** Because they have onboard hardware implementations of encryption, hashing, and key generation, they greatly simplify the use of certificate authorities and the public key infrastructure (PKI).
- **B.** As a trust root, a TPM can make hierarchies of trust more reliable.

C. The TPM replaces the host system's random number generators and hash routines with its hardware-accelerated, more secure versions. This enhances system security as well as runtime performance.

D. As a signed part of operating systems kernels, TPMs make it possible to validate software updates more reliably.

13. Which statement about how cryptography protects the meaning or content of files and messages is incorrect?

A. Cryptography obscures meaning by misdirection, concealment, or deception.

B. Cryptography obscures meaning by making it difficult or impossible for unauthorized users to access it, view it, copy it, or change it.

C. Cryptography transforms the meaning and content of a file or message into a unique value.

D. Cryptography is part of digitally signing files and messages to authenticate senders.

14. Which of the following best explains symmetric encryption?

A. Uses one key to encrypt blocks of text to be ciphered and another key to decrypt it back

B. Uses the same key or a simple transform of it to encrypt clear text into ciphertext, and then decrypt the ciphertext back into plaintext

C. Was used extensively in classical encryption but has since been superseded by much stronger asymmetric encryption

D. Is best suited to cleartext that has a very high degree of regularity to its structure and content

15. Properly used, cryptographic techniques improve all aspects of information security except:

A. Confidentiality

B. Authentication

C. Nonrepudiation

D. Accountability

16. Nonrepudiation relies on cryptography to validate that:

A. The sender or author of a document or file is who the recipient thinks it is

B. The file or message has not been tampered with during transit or storage

C. The file or message has not been viewed by others or copied without the sender's and named recipient's knowledge

D. The certificate, public key, or both associated with the sender or author match what is associated with the file or message

17. Which statement best describes how digital signatures work?

- **A.** The sender hashes the message or file to produce a message digest and applies the chosen encryption algorithm and their private key to it. This is the signature. The recipient uses the sender's public key and applies the corresponding decryption algorithm to the signature, which will produce a matching message digest only if the message or file is authentically from the sender.
- **B.** The sender hashes the message or file to produce a message digest and applies the chosen decryption algorithm and their public key to it. This is the signature. The recipient uses the sender's private key and applies the corresponding encryption algorithm to the signature, which will produce a matching message digest only if the message or file is authentically from the sender.
- **C.** The sender hashes the message or file to produce a message digest and applies the chosen decryption algorithm and their private key to it. This is the signature. The recipient uses the sender's public key and applies the corresponding encryption algorithm to the signature, which will produce a matching message digest only if the message or file is authentically from the sender.
- **D.** The sender encrypts the message or file with their private key and hashes the encrypted file to produce the signed message digest. This is the signature. The recipient uses the sender's public key and applies the corresponding decryption algorithm to the signature, which will produce a matching message digest only if the message or file is authentically from the sender.

18. Which statement about subjects and objects is not correct?

- **A.** Subjects are what users or processes require access to in order to accomplish their assigned duties.
- **B.** Objects can be people, information (stored in any fashion), devices, processes, or servers.
- **C.** Objects are the data that subjects want to access in order to read it, write to it, or otherwise use it.
- **D.** Subjects are people, devices, or processes.

19. Which statement about a reference monitor in an identity management and access control system is correct?

- **A.** It should be tamper-resistant.
- **B.** Its design and implementation should be complex so as to defeat reverse engineering attacks.
- **C.** It's an abstract design concept, which is not actually built into real hardware, operating systems, or access control implementations.
- **D.** It is part of the secure kernel in the accounting server or services provided by strong access control systems.

20. What kinds of privileges should be part of what your mandatory access control policies can grant or deny to a requesting subject? (Choose all that apply.)

- **A.** Any privilege relating to reading from, writing to, modifying or deleting the object in question if it was created or is owned by the requesting subject
- **B.** Reading or writing/modifying the metadata associated with an object
- **C.** Modifying access control system constraints, rules, or policies
- **D.** Reading, writing, deleting, or asking the system to load the object as an executable task or thread and run it

21. Which set of steps correctly shows the process of identity management?

1. Proofing
2. Provisioning
3. Review
4. Revocation
5. Deletion

- **A.** 1, 2, 3, 4, and then 5
- **B.** 2, 3, 4
- **C.** 1, 2, 4, 5
- **D.** 2, 3, 5

22. What's the least secure way to authenticate device identity prior to authorizing it to connect to the network?

- **A.** MAC address whitelisting
- **B.** Multifactor authentication that considers device identification, physical location, and other attributes
- **C.** Verifying that the device meets system policy constraints as to software and malware updates
- **D.** Devices don't authenticate, but the people using them do.

23. In access control authentication systems, which is riskier, false positive or false negative errors?

- **A.** False negative, because they lead to a threat actor being granted access
- **B.** False positive, because they lead to a threat actor being granted access
- **C.** False negative, because they lead to legitimate subjects being denied access, which impacts business processes
- **D.** False positive, because they lead to legitimate subjects being denied access, which impacts business processes

24. Which statement about single-factor versus multifactor authentication is most correct?

- **A.** Single-factor is easiest to implement but with strong authentication is the hardest to attack.
- **B.** Multifactor requires greater implementation, maintenance, and management but can be extremely hard to spoof as a result.
- **C.** Multifactor authentication requires additional hardware devices to make authentication properly secure.
- **D.** Multifactor authentication should be reserved for those high-risk functions that require extra security.

25. When comparing the TCP/IP and OSI reference model as sets of protocols, which statement is most correct?

- **A.** Network hardware and systems are built on TCP/IP, whereas the OSI reference model only provides concepts and theories.
- **B.** TCP/IP only provides concepts and theories, whereas network hardware and systems are built using the OSI reference model.
- **C.** Both sets of protocols provide theories and concepts, but real hardware is built around the data, control, and management planes.
- **D.** Hardware and systems are built using both models, and both models are vital to threat assessment and network security.

26. Is IPv6 backward compatible with IPv4?

- **A.** No, because the differences in addressing, packet header structure, and other features would not allow an IPv4 packet to successfully travel on an IPv6 network
- **B.** No, because IPv4 packets cannot meet the new security considerations built into IPv6
- **C.** Yes, because IPv6 has services built into the protocol stacks to convert IPv4 packets into IPv6 compatible structures
- **D.** Yes, because the transport and routing protocols are the same

27. Which statement about subnetting is correct?

- **A.** Subnetting applies only to IPv4 networks, unless you are using classless interdomain routing.
- **B.** Both IPv4 and IPv6 provide for subnetting, but the much larger IPv6 address field makes this a lot simpler to design and manage.
- **C.** Subnetting in IPv4 involves the CIDR protocol, which runs at Layer 3; in IPv6, this protocol, and hence subnetting, is not used.
- **D.** Because the subnet mask field is so much larger in IPv6, it is easier to subnet in this newer protocol stack than in IPv4.

28. Which statement or statements about ports and the Internet is *not* correct? (Choose all that apply.)

- **A.** Using port numbers as part of addressing and routing was necessary during the early days of the Internet, largely because of the small size of the address field, but IPv6 makes most port usage obsolete.
- **B.** Standard ports are defined for a number of protocols, and these ports allow sender and receiver to establish connectivity for specific services.
- **C.** Standardized port assignments cannot be changed, or things won't work right, but they can be mapped to other port numbers by the protocol stacks on senders' and recipients' systems.
- **D.** Many modern devices, such as those using Android, cannot support ports, and so apps have to be redesigned to use alternate service connection strategies.

29. Which of the following statements about man-in-the-middle (MITM) attacks is most correct?

- **A.** Session stealing attacks are not MITM attacks.
- **B.** MITM attacks can occur at any layer and against connectionless or connection-oriented protocols.
- **C.** This basic attack strategy can be used at any layer of the protocols where there is connection-oriented, stateful communication between nodes.
- **D.** MITM attacks can work only at Layer 4.

30. What important role does systems monitoring perform in support of incident management?

- **A.** They are not related; monitoring is a routine task that uses trend analysis and data analytics to determine whether past systems behavior and use has been within expected bounds.
- **B.** Essential; by bringing together alert and alarm indicators from systems and their associated security controls and countermeasures, monitoring is the watchdog capability that activates incident response capabilities and plans.
- **C.** Incident response includes its own monitoring and alarms capabilities, so systems monitoring provides a good backup or alternate path to determining whether an incident is occurring.
- **D.** Ongoing, continuous monitoring is used to adjust or fine-tune alarm threshold settings so that false alarm rates can be better managed.

31. How might you keep a gap from becoming a blind spot in your information security defenses?

- **A.** Transfer this risk to insurers or other parties.
- **B.** Ensure that systems elements around the gap provide sufficient detection and reporting capabilities so that an event of interest occurring in the gap cannot spread without being detected.
- **C.** Ensure that other systems elements can either detect or report when an event of interest is happening within the gap.
- **D.** You can't, as by definition the gap is where you have no appreciable security coverage, and this includes having no monitoring or detection capabilities.

32. CVE data and your own vulnerability assessments indicate that many of your end-user systems do not include recent security patches released by the software vendors. You decide to bring these systems up to date by applying these patches. This is an example of which of the following?

A. Remediating or mitigating a risk

B. Transferring a risk

C. Avoiding a risk

D. Accepting a risk

33. Which of the following might be legitimate ways to transfer a risk? (Choose all that apply.)

A. Recognize that government agencies have the responsibility to contain, control, or prevent this risk, which your taxes pay them to do.

B. Pay insurance premiums for a policy that provides for payment of claims and liabilities in the event the risk does occur.

C. Shift the affected business processes to a service provider, along with contractually making sure they are responsible for controlling that risk or have countermeasures in place to address it.

D. Change the underlying business process to use more secure software and hardware systems.

34. Which statement correctly describes why CVE data should be part of your vulnerability assessments?

A. It should provide most if not all of the vulnerability information you need to implement risk mitigation.

B. Since hackers use CVE data to aid in planning their attacks, this should be the first place you look for insight as you do emergency hardening of your IT systems. Once these obvious vulnerabilities have been mitigated, a more complete vulnerability assessment should be done.

C. It's a great source of information for known systems elements and known vulnerabilities associated with them, but it does nothing for vulnerabilities that haven't been reported yet or for company-developed IT elements.

D. Since the vast majority of systems in use are based on Windows, if your business does not use Windows platforms you can probably avoid the expense of investigating CVE for vulnerability information.

35. Which of the following activities are not part of information risk mitigation?

A. Implementing new systems features or capabilities to enhance product quality

B. Incident management and investigation, after a suspected information security breach

C. Installing and testing new firewall, switch, and router systems and settings

D. Developing an information classification policy and process

36. Which of the following shows the major steps of the information risk management process in the correct order?

- **A.** Assess risks across the organization; identify information security and privacy risks; implement countermeasures; establish security and privacy posture; review supply chain for IT security risk elements
- **B.** Establish basic security posture; review risks; implement countermeasures; ongoing monitoring and assessment; testing; training
- **C.** Set priorities; assess risks; select controls and countermeasures; implement controls; validate correct operation; monitor
- **D.** Develop business impact analysis (BIA); establish risk tolerance levels; implement damage control choices; monitor

37. What is information risk?

- **A.** The threat that your computers, online storage, or cloud-hosted or other data could be hacked into and data stolen or changed
- **B.** The probability of an event occurring that disrupts your information and the business processes and systems that use it
- **C.** Vulnerabilities in your information systems that can be exploited by a threat actor and cause harmful impacts
- **D.** The probability that management and leadership's directions and communications will be misunderstood, causing the wrong actions to be taken by stakeholders, possibly causing financial loss, injury, or death

38. Which is the most correct statement as to what it means to have a proactive approach with your information security risk management plans, programs, and systems?

- **A.** Being proactive means that your countermeasures and controls can actively trace back to identify, locate, and characterize your attackers, which can help you both in defending against them and in potentially seeking legal redress.
- **B.** Senior leaders and managers in many businesses appreciate active, thoughtful, forward-looking approaches, and you will find it easier to gain their support.
- **C.** Proactive information security systems allow your security specialists to take real-time control of all systems elements and bring all information about events of interest into one common operational picture. This greatly enhances your ability to detect, characterize, and contain incidents.
- **D.** Being proactive means that you use the best knowledge you have today, including lessons learned from other organizations' experience with information risk, and you plan ahead to use these lessons to deal with these risks them, rather than wait for them to occur and then investigate how to respond to them.

39. What kind of information is part of an information risk assessment process? (Choose all that apply.)

- **A.** Lost revenues during the downtime caused by the risk incident, including time it takes to get things back to normal
- **B.** Damage to equipment or facilities, or injury or death to people
- **C.** Estimated costs to implement chosen solutions, remediations, controls, or countermeasures
- **D.** Total costs to create an asset that is damaged or disrupted by the risk event

40. There are three ways in which risk assessments can be done. Choose the option that orders them from best to least in terms of their contribution to risk management decision making.

- **A.** Qualitative, quantitative, and CVE-based
- **B.** CVE-based, quantitative, and qualitative
- **C.** There is no order; they all can and should be used, as each reveals something more about the risks you have to manage.
- **D.** Quantitative, CVE-based, and qualitative

41. Patsy is reviewing the quantitative risk assessment spreadsheet for her division, and she sees a number of entries where the annual loss expectancy is far greater than the single loss expectancy. This suggests that:

- **A.** The RTO is later than the RPO.
- **B.** The ARO is less than 1.
- **C.** The particular risk is assessed to happen many times per year; thus its ARO is much greater than 1.
- **D.** This looks like an error in estimation or assessment, and should be further investigated.

42. Which statement is incorrect as to how you should use RTO, MAO, and RPO in planning information risk management activities?

- **A.** Return to operations (RTO) is the desired time to get all business processes back into operation, whether on backup or workaround systems or on production systems brought back to normal. The recovery priority objective (RPO) sets priorities for which systems to bring up first or which business processes to get back into operation before others (of lower priority).
- **B.** Recovery point objective (RPO) establishes the maximum amount of data that is lost due to a risk event. This could be in numbers of transactions or in units of time and indicates the amount of rework of information that is acceptable to get systems back into normal operation.
- **C.** Recovery time objective (RTO) must be less than or equal to the maximum acceptable outage. MAO sets a maximum down time (outage time) before mission impact becomes unacceptable; RTO can be used to emphasize faster-than-MAO restoration.
- **D.** Maximum acceptable outage (MAO) relates to the mission or business objectives; if multiple systems support those objectives, then all of their recovery time objectives (RTOs) must be less than or equal to the MAO.

43. What are all of the choices we need to make when considering information risk management, and what's the correct order to do them in?

1. Treatment: accept, treat (fix or mitigate), transfer, avoid, recast
2. Damage limitation: deter, detect, prevent, avoid
3. Perspective: outcomes, assets, process or threat based
4. Impact assessment: quantitative or qualitative

A. 1, 2, 3, then 4

B. 3, 4, 2, then 1

C. 4, 3, 2, then 1

D. 2, 3, 1 then 4

44. What do we use protocols for? (Choose all that apply.)

A. To conduct ceremonies, parades, or how we salute superiors, sovereigns, or rulers

B. To have a conversation with someone, and keep disagreement from turning into hostile, angry argument

C. To connect elements of computer systems together so that they can share tasks and control each other

D. As abstract design tools when we are building systems, but we don't actually build hardware or software that implements a protocol

E. None of the above

45. As an SSCP, you work at the headquarters of a retail sales company that has many stores around the country. Its training department has prepared different training materials and operations manuals for in-store sales, warehouse staff, and other team members to use in their jobs. Almost all of these describe procedures that people do as they work with each other or with customers. From an information security standpoint, which of the following statements is correct?

A. Since these all describe people-to-people interactions and processes, they are not implemented by the IT department, and so they're not something that information security is concerned with.

B. Most of their content is probably common practice in business and retail sales and so would not be trade secrets, company proprietary, or private to the company.

C. Although these processes are not implemented in IT systems, the documents and videos themselves are hosted in company-provided IT systems, and so information security requirements apply.

D. If the company has decided that the content of these training materials is proprietary or company confidential, then their confidentiality must be protected. They must also be protected from tampering or unauthorized changes and be available to staff in the stores to use when they need them if the company is to do business successfully. Therefore, information security applies.

46. We often hear people talk about the need for information systems to be safe and reliable. Is this the same as saying that they need to be secure?

A. No, because reliability has to do with failures of equipment, errors in software design or use, or bad data used as input, whereas security is focused on keeping the systems and their data safe from intrusion or unwanted change.

B. Yes, because the objective of information security is to increase our confidence that we can make sound and prudent decisions based on what those information systems are telling us and, in doing so, cause no harm.

C. Yes, because all information and information systems are built by humans, and humans make mistakes, so we need strong safety rules and procedures to keep from causing harm.

D. No, but they have ideas in common. For example, data integrity can lead to unsafe operation, but information security by itself cannot identify possible safety consequences.

47. Due diligence means which of the following?

A. Pay your debts completely, on time.

B. Do what you have to do to fulfill your responsibilities.

C. Make sure that actions you've taken to fulfill your responsibilities are working correctly and completely.

D. Read and review the reports from subordinates or from systems monitoring data.

48. Protection of intellectual property (IP) is an example of what kind of information security need?

A. Privacy

B. Confidentiality

C. Availability

D. Integrity

49. A thunderstorm knocks out the commercial electric power to your company's datacenter, shutting everything down. This impacts which aspect of information security?

A. Privacy

B. Confidentiality

C. Integrity

D. Availability

50. Explain the relationship between confidentiality and privacy, if any:

A. Confidentiality is about keeping information secret so that we retain advantage or do not come to harm; privacy is about choosing who can enter one's life or property.

B. Confidential information is information that must be kept private, so they really have similar meanings.

C. Privacy laws allow criminals to hide their actions and intentions from society, but confidentiality allows for the government to protect defense-related information from being leaked to our enemies.

D. Confidentiality is the freedom to choose whom we share information with; privacy refers to information that is specifically about our individual lives, activities, or interests.