ISC2

Mike Chapple, CISSP
David Seidl, CISSP

CISSP®

Certified Information
Systems Security Professional

# OFFICIAL PRACTICE TESTS

**Fourth Edition**

Provides four complete, unique practice tests and 100 additional questions per domain covering all current CISSP exam objectives

Complements the Sybex *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide, Tenth Edition*

SYBEX®
A Wiley Brand

# ISC2® CISSP®

# Certified Information Systems Security Professional

## Official Practice Tests

### Fourth Edition

# ISC2® CISSP®

# Certified Information Systems Security Professional

## Official Practice Tests

**Fourth Edition**

Mike Chapple, CISSP

David Seidl, CISSP

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394255078 (paperback), 9781394255092 (ePDF), 9781394255085 (ePub)



**Library of Congress Cataloging in Publication data available on request.**

Cover image: © Getty Images Inc./Jeremy Woodhouse

Cover design: Wiley

# Acknowledgments

The authors would like to thank the many people who made this book possible. Jim Minatel at Wiley Publishing helped us extend the Sybex CISSP franchise to include this title and has continued to champion the International Information System Security Certification Consortium (ISC2). Carole Jelen, our agent, tackles all the back-end magic for our writing efforts and worked on both the logistical details and the business side of the book with her usual grace and commitment to excellence. Aaron Kraus, Shahla Pirnia, and Emily Vandewater, our technical editors, pointed out many opportunities to improve our work and deliver a high-quality final product. Kelly Talbot served as our project manager and made sure everything fit together. Many other people we'll never meet worked behind the scenes to make this book a success, and we really appreciate their time and talents to make this next edition come together.

# About the Authors

**Mike Chapple, PhD, CISSP,** is an author of the best-selling ISC2 CISSP *Certified Information Systems Security Professional Official Study Guide* (Sybex, 2024), now in its 10th edition. He is an information security professional with more than 25 years of experience in higher education, the private sector, and government.

Mike is currently a teaching professor of IT, analytics, and operations at the University of Notre Dame's Mendoza College of Business. He previously was a senior director for IT service delivery at Notre Dame, where he oversaw the information security, data governance, IT architecture, project management, strategic planning, and product management functions for the university.

Before returning to Notre Dame, Mike served as the executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active-duty intelligence officer in the U.S. Air Force.

Mike earned both his BS and PhD degrees from Notre Dame in computer science and engineering. He also holds an MS in computer science from the University of Idaho and an MBA from Auburn University. His IT certifications include the CISSP, Security+, CySA+, CISA, PenTest+, CIPP/US, CISM, CCSP, and PMP credentials.

Mike is the author of more than 100 technology books and video courses focused on security and privacy certifications. He provides books, video-based training, and free study groups for a wide variety of IT certifications at his website, `CertMike.com`.

**David Seidl, CISSP,** is the vice president for information technology and CIO at Miami University where he leads a nationally recognized and award-winning IT organization. During his IT career, he has served in a variety of technical and information security roles including as the senior director for Campus Technology Services at the University of Notre Dame where he co-led Notre Dame's move to the cloud and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and services. He also served as Notre Dame's director of information security. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business and has written more than 20 books on security certification and cyberwarfare, including coauthoring the previous editions of *CISSP ISC2 Official Practice Tests* (Sybex, 2021) as well as *CompTIA CySA+ Study Guide: Exam CS0-003*, *CompTIA CySA+ Practice Tests: Exam CS0-003*, *CompTIA Security+ Study Guide: Exam SY0-701*, and *CompTIA Security+ Practice Tests: Exam SY0-701* as well as other certification guides and books on information security.

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as CISSP, CySA+, PenTest+, GPEN, and GCIH certifications.

# About the Technical Editors

**Aaron Kraus, CISSP, CCSP,** began his career as a security auditor and has gone on to work in security and compliance roles across financial services, insurance, consulting, and tech start-ups. He is currently a senior consultant at Latacora and runs his own consulting business, with experience ranging from initial implementation to aligning large, multinational organization's security programs to meet evolving compliance needs, respond to emerging threats, and accommodate new and changing business practices. He has been a course author, instructor, and dean of cybersecurity curriculum at Learning Tree International for more than 15 years and has worked on several publications at Wiley. He is the author of *The Official ISC2 CCSP CBK Reference, 4th Edition*, and coauthor of *The Official ISC2 CISSP CBK Reference, 6th Edition*, as well as the technical editor for the official CISSP and CCSP study guides and practice test books.

**Shahla Pirnia** is a freelance technical editor and proofreader with a focus on cybersecurity and certification topics. She currently serves as a technical editor for `CertMike.com`. Shahla earned BS degrees in computer and information science and Psychology from UMGC and an AA in information systems from Montgomery College, MD. Shahla's IT certifications include CompTIA Security+, Network+, A+, and ISC2 CC.

**Emily Vandewater** is a senior principal security consultant at Elteni Cybersecurity Consulting and Advisory, where she focuses on building information security programs and providing strategic guidance to mitigate cyber risks and ensure regulatory compliance. With more than 15 years of progressive experience in the tech and cybersecurity sectors, Emily has distinguished herself through key leadership positions, notably as a former director of information security at an IT managed service provider. Beyond her consulting work, Emily applies her expertise as a freelance technical editor and content developer for leading publishers, including Wiley. Her deep understanding of cybersecurity is backed by an array of IT certifications, including ISC2 CISSP and SSCP, CompTIA CASP+, CySA+, Security+ and Cloud+, Azure, and Microsoft Administrator Expert.

# Contents

# Introduction

*ISC2 CISSP® Certified Information Systems Security Professional Official Practice Tests Fourth Edition* is a companion volume to *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide, Tenth edition* (*Sybex, 2024*). It includes questions that cover content from the CISSP Detailed Content Outline and exam that became effective on April 15, 2024. If you're looking to test your knowledge before you take the CISSP exam, this book will help you by providing more than 1,300 questions that cover the CISSP Common Body of Knowledge (CBK) and easy-to-understand explanations of both right and wrong answers.

If you're just starting to prepare for the CISSP exam, we highly recommend that you use the *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide* to help you learn about each of the domains covered by the CISSP exam. Once you're ready to test your knowledge, use this book to help find places where you may need to study more or to practice for the exam itself.

Since this is a companion to the *CISSP Study Guide*, this book is designed to be similar to taking the CISSP exam. It contains multipart scenarios as well as standard multiple-choice and matching questions like you may encounter on the certification exam. The book is broken up into 12 chapters: 8 domain-centric chapters with 100 or more questions about each domain, and 4 chapters that contain 125-question practice tests to simulate taking the exam.

# CISSP Certification

The CISSP certification is offered by the International Information System Security Certification Consortium (ISC2), a global nonprofit organization. ISC2's mission statement says that "ISC2 strengthens the influence, diversity and vitality of the field through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world." ISC2 achieves this mission by delivering the world's leading information security certification program, the CISSP. ISC2 also offers additional certifications including the following:

- Certified in Cybersecurity (CC)
- Systems Security Certified Practitioner (SSCP)
- Certified Cloud Security Professional (CCSP)
- Governance, Risk and Compliance Certification (CGRC)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Information Systems Security Architecture Professional (ISSAP)
- Information Systems Security Engineering Professional (ISSEP)
- Information Systems Security Management Professional (ISSMP)

The CISSP certification covers eight domains of information security knowledge. These domains are meant to serve as the broad knowledge foundation required to succeed in the information security profession.

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

The CISSP domains are periodically updated by ISC2. The most recent revision on April 15, 2024, slightly modified the weighting for Security and Risk Management from 15% to 16%, while decreasing the focus on Software Development Security from 11% to 10%. It also added or expanded coverage of topics such as intellectual property, privacy laws and regulations, software bills of materials, end-of-life support, SASE, operational technology, high-performance computing, intermediate distribution frame, Compute Express Link, and a variety of other topics.

Complete details on the CISSP CBK are contained in the 2024 CISSP Detailed Content Outline. It includes a full outline of exam topics, which can be found on the ISC2 website at `www.isc2.org`.

# Taking the CISSP Exam

The English version of the CISSP exam uses a technology called *computerized adaptive testing* (CAT). With this format, you will face an exam containing between 100 to 150 questions with a three-hour time limit. You will not have the opportunity to skip back and forth because the computer selects the next questions that it asks you based upon your answers to previous questions. If you're doing well on the exam, it will get more difficult as you progress. Don't let that unnerve you!

You can find more information about computerized adaptive testing directly from ISC2 at `www.isc2.org/certifications/cissp/cissp-cat`.

The computerized adaptive testing version of the exam is offered in English, Chinese, German, Japanese, and Spanish. Unlike earlier versions of the exam, the CISSP exam will no longer be offered in linear exam format after April 15th, 2024.

While it's impossible to directly simulate a CAT exam in book form, as you work through these practice exams you might want to use 80% as a goal to help you get a sense of whether you're ready to sit for the actual exam. When you're ready, you can schedule an exam at a location near you through the ISC2 website.

Questions on the CISSP exam are provided in both multiple-choice form and what ISC2 calls *advanced innovative* questions, which are drag-and-drop and hotspot questions, both of which are offered in a computer-based testing environment. Innovative questions are scored the same as traditional multiple-choice questions and have only one right answer.

ISC2 exam policies are subject to change. Please be sure to check www.isc2.org for the current policies before you register and take the exam.

# Computer-Based Testing Environment

CISSP exams are administered in a computerized adaptive testing (CAT) format. You'll start the registration for your exam through your ISC2 login at `www.isc2.org/register-for-exam`. You may take the exam at a Pearson VUE authorized center in the language of your choice. It is offered in English, Chinese, German, Japanese, and Spanish.

You'll take the exam in a computer-based testing center located near your home or office. The centers administer many different exams, so you may find yourself sitting in the same room as a student taking a school entrance examination and a healthcare professional earning a medical certification. If you'd like to become more familiar with the testing environment, the Pearson VUE website offers a virtual tour of a testing center.

```
https://home.pearsonvue.com/Test-takers/
Pearson-Professional-Center-tour.aspx
```

When you take the exam, you'll be seated at a computer that has the exam software already loaded and running. It's a pretty straightforward interface that allows you to navigate through the exam. You can download a practice exam and tutorial from the Pearson VUE website.

```
https://home.pearsonvue.com
```

Like all exams, the CISSP certification from ISC2 is updated periodically and may eventually be retired or replaced. At some point after ISC2 is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired, or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

# Exam Retake Policy

If you don't pass the CISSP exam, you shouldn't panic. Many individuals don't reach the bar on their first attempt but gain valuable experience that helps them succeed the second time around. When you retake the exam, you'll have the benefit of familiarity with the exam environment and CISSP CAT exam format. You'll also have time to study the areas where you felt less confident.

After your first exam attempt, you must wait 30 days before retaking the computer-based exam. If you're not successful on that attempt, you may re-test after 60 days. If you don't pass after your third attempt, you can re-test after 90 days for that and any subsequent attempts. You can't take the test more than 4 times within a 12-month period. You can obtain more information about ISC2 and its other certifications from its website at `www.isc2.org`.

# Work Experience Requirement

Candidates who want to earn the CISSP credential must not only pass the exam but also demonstrate that they have at least five years of work experience in the information security field. Your work experience must cover activities in at least two of the eight domains of the CISSP exam outline and must be paid, full-time or qualified part-time employment or paid or unpaid internship. Volunteer experiences are not acceptable to meet the CISSP experience requirement.

You may be eligible to waive one of the five years of the work experience requirement based upon your educational achievements. If you hold a bachelor's degree or four-year equivalent, you may be eligible for a degree waiver that covers one of those years. Similarly, if you hold one of the information security certifications on the current ISC2 approved credential list (`www.isc2.org/certifications/cissp/cissp-experience-requirements`), you may also waive a year of the experience requirement. You may not combine these two programs. Holders of both a certification and an undergraduate degree must still demonstrate at least four years of experience.

If you haven't yet completed your work experience requirement, you may still attempt the CISSP exam. Individuals who pass the exam are designated Associates of ISC2 and have six years to complete the work experience requirement.

# Recertification Requirements

Once you've earned your CISSP credential, you'll need to maintain your certification by paying maintenance fees and participating in continuing professional education (CPE). As long as you maintain your certification in good standing, you will not need to retake the CISSP exam.

Currently, the annual maintenance fees for the CISSP credential are $135 per year. This fee covers the renewal for all ISC2 certifications held by an individual.

The CISSP CPE requirement mandates earning at least 120 CPE credits during each three-year renewal cycle. Associates of ISC2 must earn at least 15 CPE credits each year. ISC2 provides an online portal where certificate holders may submit CPE completion for review and approval. The portal also tracks annual maintenance fee payments and progress toward recertification.

# Using This Book to Practice

This book is composed of 12 chapters. Each of the first eight chapters covers a domain, with a variety of questions that can help you test your knowledge of real-world, scenario, and security best-practices. The final four chapters are complete practice exams that can serve as timed practice tests to help determine whether you're ready for the CISSP exam.

We recommend taking the first practice exam to help identify where you may need to spend more study time and then using the domain-specific chapters to test your domain knowledge where it is weak. Once you're ready, take the other practice exams to make sure you've covered all the material and are ready to attempt the CISSP exam.

# Using the Online Practice Tests

All the questions in this book are also available in Sybex's online practice test tool. To get access to this online format, go to `www.wiley.com/go/sybextestprep` and start by registering your book. You'll receive a PIN and instructions on where to create an online test bank account. Once you have access, you can use the online version to create your own sets of practice tests from the book questions and practice in a timed and graded setting.

# How to Contact the Publisher

If you believe you have found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

Chapter 1

# Security and Risk Management (Domain 1)

## SUBDOMAINS

- ✓ 1.1 Understand, adhere to, and promote professional ethics
- ✓ 1.2 Understand and apply security concepts
- ✓ 1.3 Evaluate, apply, and sustain security governance principles
- ✓ 1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context
- ✓ 1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
- ✓ 1.6 Develop, document, and implement security policy, standards, procedures, and guidelines
- ✓ 1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements
- ✓ 1.8 Contribute to and enforce personnel security policies and procedures
- ✓ 1.9 Understand and apply risk management concepts
- ✓ 1.10 Understand and apply threat modeling concepts and methodologies
- ✓ 1.11 Apply Supply Chain Risk Management (SCRM) concepts
- ✓ 1.12 Establish and maintain a security awareness, education, and training program

1. Alyssa is responsible for her organization's security awareness program. She is concerned that changes in technology may make the content outdated. What control can she put in place to protect against this risk?
   - **A.** Gamification
   - **B.** Computer-based training
   - **C.** Content reviews
   - **D.** Live training

2. Gavin is creating a report for management on the results of his most recent risk assessment. In his report, he would like to identify the remaining level of risk to the organization after adopting security controls. What term best describes this current level of risk?
   - **A.** Inherent risk
   - **B.** Residual risk
   - **C.** Control risk
   - **D.** Mitigated risk

3. Francine is a security specialist for an online service provider in the United States. She recently received a claim from a copyright holder that a user is storing information on her service that violates the third party's copyright. What law governs the actions that Francine must take?
   - **A.** Copyright Act
   - **B.** Lanham Act
   - **C.** Digital Millennium Copyright Act
   - **D.** Gramm-Leach-Bliley Act

4. FlyAway Travel has offices in both the European Union (EU) and the United States and transfers personal information between those offices regularly. They have recently received a request from an EU customer requesting that their account be terminated. Under the General Data Protection Regulation (GDPR), which requirement for processing personal information states that individuals may request that their data no longer be disseminated or processed?
   - **A.** The right to access
   - **B.** Privacy by Design
   - **C.** The right to erasure
   - **D.** The right of data portability

5. After conducting a qualitative risk assessment of her organization, Sally recommends purchasing cybersecurity breach insurance. What type of risk response behavior is she recommending?
   - **A.** Accept
   - **B.** Transfer
   - **C.** Reduce
   - **D.** Reject

6. Which one of the following elements of information is not considered personally identifiable information that would trigger most United States state data breach laws?
   - **A.** Student identification number
   - **B.** Social Security number
   - **C.** Driver's license number
   - **D.** Credit card number

7. Renee is purchasing a new software product and is working with the vendor on the negotiation of a license agreement that will specify customized terms of use and a discounted price. What type of agreement would normally be used to document the results of this negotiation?
   - **A.** Perpetual license
   - **B.** Subscription license
   - **C.** Enterprise license agreement
   - **D.** End-user license agreement

8. Henry recently assisted one of his co-workers in preparing for the CISSP® exam. During this process, Henry disclosed confidential information about the content of the exam, in violation of Canon IV of the Code of Ethics: "Advance and protect the profession." Who may bring ethics charges against Henry for this violation?
   - **A.** Anyone may bring charges.
   - **B.** Any certified or licensed professional may bring charges.
   - **C.** Only Henry's employer may bring charges.
   - **D.** Only the affected employee may bring charges.

9. Wanda is working with one of her organization's European Union business partners to facilitate the exchange of customer information. Wanda's organization is located in the United States. What would be the best method for Wanda to use to ensure GDPR compliance?
   - **A.** Binding corporate rules
   - **B.** Privacy Shield
   - **C.** Standard contractual clauses
   - **D.** Safe harbor

10. Yolanda is the chief privacy officer for a financial institution and is researching privacy requirements related to customer checking accounts. Which one of the following laws is most likely to apply to this situation?
    - **A.** GLBA
    - **B.** SOX
    - **C.** HIPAA
    - **D.** FERPA

**11.** Tim's organization recently received a contract to conduct sponsored research as a government contractor. What law now likely applies to the information systems involved in this contract?

**A.** FISMA

**B.** PCI DSS

**C.** HIPAA

**D.** GISRA

**12.** Chris is advising travelers from his organization who will be visiting many different countries overseas. He is concerned about compliance with export control laws. Which of the following technologies is most likely to trigger these regulations?

**A.** Memory chips

**B.** Office productivity applications

**C.** Hard drives

**D.** Encryption software

**13.** Bobbi is investigating a security incident and discovers that an attacker began with a normal user account but managed to exploit a system vulnerability to provide that account with administrative rights. What type of attack took place under the STRIDE threat model?

**A.** Spoofing

**B.** Repudiation

**C.** Tampering

**D.** Elevation of privilege

**14.** You are completing your business continuity planning effort and have decided that you want to accept one of the risks. What should you do next?

**A.** Implement new security controls to reduce the risk level.

**B.** Design a disaster recovery plan.

**C.** Repeat the business impact assessment.

**D.** Document your decision-making process.

**15.** You are completing a review of the controls used to protect a media storage facility in your organization and would like to properly categorize each control that is currently in place. Which of the following control categories accurately describe a fence around a facility? (Select all that apply.)

**A.** Physical

**B.** Detection

**C.** Deterrent

**D.** Preventive

**16.** Tony is developing a business continuity plan and is having difficulty prioritizing resources because of the difficulty of combining information about tangible and intangible assets. What would be the most effective risk assessment approach for him to use?

**A.** Quantitative risk assessment

**B.** Qualitative risk assessment

**C.** Neither quantitative nor qualitative risk assessment

**D.** Combination of quantitative and qualitative risk assessment

**17.** Vincent believes that a former employee took trade secret information from his firm and brought it with him to a competitor. He wants to pursue legal action. Under what law could he pursue charges?

**A.** Copyright law

**B.** Lanham Act

**C.** Glass-Steagall Act

**D.** Economic Espionage Act

**18.** Which one of the following principles imposes a standard of care upon an individual that is broad and equivalent to what one would expect from a reasonable person under the circumstances?

**A.** Due diligence

**B.** Separation of duties

**C.** Due care

**D.** Least privilege

**19.** Brenda's organization recently completed the acquisition of a competitor firm. Which one of the following tasks would be LEAST likely to be part of the organizational processes addressed during the acquisition?

**A.** Consolidation of security functions

**B.** Integration of security tools

**C.** Protection of intellectual property

**D.** Documentation of security policies

**20.** Kelly believes that an employee engaged in the unauthorized use of computing resources for a side business. After consulting with management, she decides to launch an administrative investigation. What is the burden of proof that she must meet in this investigation?

**A.** Preponderance of the evidence.

**B.** Beyond a reasonable doubt.

**C.** Beyond the shadow of a doubt.

**D.** There is no standard.

**21.** Keenan Systems recently developed a new manufacturing process for microprocessors. The company wants to license the technology to other companies for use but wants to prevent unauthorized use of the technology. What type of intellectual property protection is best suited for this situation?

**A.** Patent

**B.** Trade secret

**C.** Copyright

**D.** Trademark

**22.** Which one of the following actions might be taken as part of a business continuity plan?

**A.** Restoring from backup tapes

**B.** Implementing RAID

**C.** Relocating to a cold site

**D.** Restarting business operations

**23.** When developing a business impact analysis, the team should first create a list of assets. What should happen next?

**A.** Identify vulnerabilities in each asset.

**B.** Determine the risks facing the asset.

**C.** Develop a value for each asset.

**D.** Identify threats facing each asset.

**24.** Mike recently implemented an intrusion prevention system designed to block common network attacks from affecting his organization. What type of risk management strategy is Mike pursuing?

**A.** Risk acceptance

**B.** Risk avoidance

**C.** Risk mitigation

**D.** Risk transference

**25.** Laura has been asked to perform a security controls assessment (SCA). What type of organization is she most likely in?

**A.** Higher education

**B.** Banking

**C.** Government

**D.** Healthcare

**26.** Carl is a federal agent investigating a computer crime case. He identified an attacker who engaged in illegal conduct and wants to pursue a case against that individual that will lead to imprisonment. What standard of proof must Carl meet?

**A.** Beyond the shadow of a doubt

**B.** Preponderance of the evidence

**C.** Beyond a reasonable doubt

**D.** Majority of the evidence

**27.** ISC2 uses the logo shown here to represent itself online and in a variety of forums. What type of intellectual property protection can it use to protect its rights in this logo?


*Source:* ISC2, Inc.

**A.** Copyright

**B.** Patent

**C.** Trade secret

**D.** Trademark

**28.** Mary is helping a computer user who sees the following message appear on his computer screen. What type of attack has occurred?


*Source:* CryptoLocker

**A.** Availability

**B.** Confidentiality

**C.** Disclosure

**D.** Distributed

**29.** Which one of the following organizations would not be automatically subject to the privacy and security requirements of HIPAA if they engage in electronic transactions?

**A.** Healthcare provider

**B.** Health and fitness application developer

**C.** Health information clearinghouse

**D.** Health insurance plan

**30.** John's network begins to experience symptoms of slowness. Upon investigation, he realizes that the network is being bombarded with TCP SYN packets and believes that his organization is the victim of a denial-of-service attack. What principle of information security is being violated?

**A.** Availability

**B.** Integrity

**C.** Confidentiality

**D.** Denial

**31.** Renee is designing a long-term security plan for her organization and has a three- to five-year planning horizon. Her primary goal is to align the security function with the broader plans and objectives of the business. What type of plan is she developing?

**A.** Operational

**B.** Tactical

**C.** Summary

**D.** Strategic

**32.** Gina is working to protect a logo that her company will use for a new product they are launching. She has questions about the intellectual property protection process for this logo. What U.S. government agency would be best able to answer her questions?

**A.** USPTO

**B.** Library of Congress

**C.** NSA

**D.** NIST

**33.** The Acme Widgets Company is putting new controls in place for its accounting department. Management is concerned that a rogue accountant may be able to create a new false vendor and then issue checks to that vendor as payment for services that were never rendered. What security control can best help prevent this situation?

**A.** Mandatory vacation

**B.** Segregation of duties

**C.** Defense in depth

**D.** Job rotation

**34.** Which one of the following categories of organizations is most likely to be covered by the provisions of FISMA?

**A.** Banks

**B.** Defense contractors

**C.** School districts

**D.** Hospitals

**35.** Robert is responsible for securing systems used to process credit card information. What security control framework should guide his actions?

**A.** HIPAA

**B.** PCI DSS

**C.** SOX

**D.** GLBA

**36.** Which one of the following individuals is normally responsible for fulfilling the operational data protection responsibilities delegated by senior management, such as validating data integrity, testing backups, and managing security policies?

**A.** Data custodian

**B.** Data owner

**C.** User

**D.** Auditor

**37.** Alan works for an e-commerce company that recently had some content stolen by another website and republished without permission. What type of intellectual property protection would best preserve Alan's company's rights?

**A.** Trade secret

**B.** Copyright

**C.** Trademark

**D.** Patent

**38.** Florian receives a flyer from a U.S. federal government agency announcing that a new administrative law will affect his business operations. Where should he go to find the text of the law?

**A.** U.S. Code

**B.** Supreme Court rulings

**C.** Code of Federal Regulations

**D.** Compendium of Laws

**39.** Tom enables an application firewall provided by his cloud infrastructure as a service provider that is designed to block many types of application attacks. When viewed from a risk management perspective, what metric is Tom attempting to lower by implementing this countermeasure?

**A.** Impact

**B.** RPO

**C.** MTO

**D.** Likelihood

**40.** Which one of the following individuals would be the most effective organizational owner for an information security program?

**A.** CISSP-certified analyst

**B.** Chief information officer (CIO)

**C.** Manager of network security

**D.** President and CEO

**41.** What important function do senior managers normally fill on a business continuity planning team?

**A.** Arbitrating disputes about criticality

**B.** Evaluating the legal environment

**C.** Training staff

**D.** Designing failure controls

**42.** You are the CISO for a major hospital system and are preparing to sign a contract with a software-as-a-service (SaaS) email vendor. You want to perform a control assessment to ensure that its business continuity planning measures are reasonable. What type of audit might you request to meet this goal?

**A.** SOC 1

**B.** FISMA

**C.** PCI DSS

**D.** SOC 2