The CISSP student guide provides a comprehensive review of the knowledge required to effectively design, engineer, and manage the overall security posture of an organization.
Dear Seminar Participant,

Congratulations! You are embarking on a journey to become part of the global (ISC)² community. Not only are you taking a critical step in your career, you are also taking an active role in inspiring a safe and secure cyber world.

Earning the CISSP certification demonstrates your ability to design and manage nearly all aspects of an organization’s cybersecurity strategy.

The material in this course is based upon the knowledge found in the (ISC)² CISSP Common Body of Knowledge. Successful completion of this course will help you achieve your career goals, but passing the CISSP exam depends on your mastery of the domains covered within the exam outline and your ability to apply those concepts in the real world.

I wish you the best of luck during the seminar and as you continue your journey to become a certified member of (ISC)².

Sincerely,

David Shearer, CISSP
Chief Executive Officer
(ISC)²
The development of the CISSP Training Guide could not have been possible without the participation and assistance of so many people. Their contributions are sincerely appreciated and gratefully acknowledged.

Authors:
Mr. Ben Malisow, CCSP and CISSP
Mr. John Berti, CCSP, CISSP, and SSCP
Dr. Lyron Andrews, CCSP and CISSP
Mr. Kevin Stoffell, CAP, CCSP, CISSP, CISSP-ISSAP, CISSP-ISSEP, and CISSP-ISSMP

Editorial Service:
Six Red Marbles
Elsa Peterson Ltd.
Mr. Dennis Lee

Instructional and Graphic Design:
Six Red Marbles

Design Oversight:
Mr. Jon Harrison, (ISC)²

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the authors and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Please be advised that among the sources of quoted material in this document are United States government publications, which by law belong to the public domain and therefore require no copyright permission or acknowledgment. Further information about copyright is available from the U.S. Copyright Office http://www.copyright.gov.

No part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system without written permission from the publishers.
# Table of Contents

Welcome ................................................................. vii

Domain 1: Security and Risk Management ........................................ 1
  Module 1: Concepts of Confidentiality, Integrity, and Availability ........ 5
  Module 2: Organizational/Corporate Governance .......................... 7
  Module 3: Risk Management Concepts ...................................... 16
  Module 4: Compliance Requirements .......................................... 38
  Module 5: Legal and Regulatory Issues that Pertain to Information Security in a Global Context ........................................... 45
  Module 6: Security Policy, Standards, Procedures, and Guidelines .......... 54
  Module 7: Personnel Security Policies and Procedures ..................... 58
  Module 8: Security Awareness, Education, and Training Programs ........ 64
  Module 9: Business Continuity Requirements .................................. 68
  Module 10: Professional Ethics ................................................. 72
  Module 11: Domain Review ..................................................... 78

Domain 2: Asset Security ...................................................... 93
  Module 1: Information and Assets ............................................. 97
  Module 2: Asset Lifecycle .................................................... 103
  Module 3: Information and Asset Ownership ................................ 117
  Module 4: Protect Privacy ..................................................... 123
  Module 5: Asset Retention .................................................... 130
  Module 6: Data Security Controls ............................................ 139
  Module 7: Information and Asset Handling Requirements ................ 165
  Module 8: Data Remanence .................................................... 169
  Module 9: Domain Review .................................................... 175
# Table of Contents

## Domain 3: Security Architecture and Engineering .......................... 189

- Module 1: Processes Using Secure Design Principles .................. 193
- Module 3: Select Controls Based upon System Security Requirements ... 205
- Module 4: Security Capabilities of Information Systems ............. 209
- Module 5: Vulnerabilities of Security Architectures, Designs, and Solution Elements ... 220
- Module 6: Cryptography ................................................. 240
- Module 7: Physical Security ............................................ 300
- Module 8: Domain Review ............................................... 316

## Domain 4: Communication and Network Security ..................... 331

- Module 1: Secure Design Principles in Network Architectures ....... 334
- Module 2: OSI Layer 1: Physical Layer ................................ 339
- Module 3: OSI Layer 2: Data-Link Layer ............................. 353
- Module 4: OSI Layer 3: Network Layer ............................... 359
- Module 5: OSI Layer 4: Transport Layer ............................. 365
- Module 6: OSI Layer 5: Session Layer ................................. 368
- Module 7: OSI Layer 6: Presentation Layer ............................ 370
- Module 8: OSI Layer 7: Application Layer ............................ 373
- Module 9: Service Considerations .................................... 378
- Module 10: Secure Network Components ............................... 383
- Module 11: Secure Communications Channels According to Design ... 389
- Module 12: Domain Review ............................................. 402

## Domain 5: Identity and Access Management (IAM) ..................... 419

- Module 1: Control Physical and Logical Access to Assets ............ 422
- Module 2: Identity and Access Provisioning Lifecycle ................ 428
- Module 3: Identification and Authentication of People, Devices, and Services 433
## Module 4: Identity Management Implementation

440

## Module 5: Implement and Manage Authorization Mechanisms

445

## Module 6: Accountability

448

## Module 7: Domain Review

450

## Domain 6: Security Assessment and Testing

465

- **Module 1: Design and Validate Assessment, Test, and Audit Strategies**
  468

- **Module 2: Security Control Testing**
  472

- **Module 3: Security Process Data**
  490

- **Module 4: Test Output and Generate Report**
  496

- **Module 5: Conduct or Facilitate Security Audits**
  498

- **Module 6: Domain Review**
  506

## Domain 7: Security Operations

521

- **Module 1: Foundational Security Operations Concepts**
  525

- **Module 2: Securely Provisioning Resources**
  531

- **Module 3: Resource Protection Techniques**
  539

- **Module 4: Detective and Preventative Measures**
  543

- **Module 5: Incident Management**
  549

- **Module 6: Requirements for Investigation Types**
  556

- **Module 7: Investigations**
  561

- **Module 8: Logging and Monitoring Activities**
  570

- **Module 9: Recovery Strategies**
  577

- **Module 10: Disaster Recovery Processes**
  586

- **Module 11: Business Continuity Planning and Exercises**
  593

- **Module 12: Test Disaster Recovery Plans**
  595

- **Module 13: Personnel Safety and Security Concerns**
  599

- **Module 14: Domain Review**
  603
## Table of Contents

**Domain 8: Software Development Security** ........................................... 615

- Module 1: Security in the Software Development Lifecycle (SDLC) ............. 619
- Module 2: Secure Coding Guidelines and Standards .................................. 642
- Module 3: Security Controls in Development Environments ....................... 685
- Module 4: The Effectiveness of Software Security .................................... 736
- Module 5: Domain Review ....................................................................... 749

**Glossary** ......................................................................................... 763

**Copyright Acknowledgments** ......................................................... 780
The Official (ISC)² Certified Information Systems Security Professional (CISSP) Training Seminar provides a comprehensive review of information systems security concepts and industry best practices, covering the eight domains of the CISSP Common Body of Knowledge (CBK):

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

This training course will help candidates review and refresh their information security knowledge as they pursue the CISSP certification.

**How Do I Use the Course Materials?**

The CISSP Training Seminar course material is built using the topics from the Exam Outline and additional topics approved by the (ISC)² CISSP Education Committee. The seminar is broken into progressively smaller sections in support of the course objectives. Each domain header identifies the objectives and what a student can expect to learn after completing the domain. These objectives are divided into smaller modules and sections. Modules contain activities that reinforce covered topics with a goal to increase knowledge retention.

The student guide is designed to be a self/group study tool that includes activities, references to external reading resources, study questions, and a glossary of terms. The columns on the outside of the pages are intended to be a place to make notes. There are three icons in use throughout the book. The icons and their meaning are outlined below.
Course Objectives

After completing this course, the participant will be able to:

1. Understand and apply fundamental concepts and methods related to the fields of information technology and security.
2. Align overall organizational operational goals with security functions and implementations.
3. Understand how to protect assets of the organization as they go through their lifecycle.
4. Understand the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.
5. Implement system security through the application of security design principals and the application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures.
6. Understand the importance of cryptography and the security services it can provide in today’s digital and information age.
7. Understand the impact of physical security elements on information system security and apply secure design principals to evaluate or recommend appropriate physical security protections.
8. Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function.
9. List the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1–7.
10. Identify standard terms for applying physical and logical access controls to environments related to their security practice.

11. Appraise various access control models to meet business security requirements.

12. Name primary methods for designing and validating test and audit strategies that support business requirements.

13. Enhance and optimize an organization’s operational function and capacity by applying and utilizing appropriate security controls and countermeasures.

14. Recognize risks to an organization’s operational endeavors, and assess specific threats, vulnerabilities, and controls.

15. Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it, and identify which security control(s) are appropriate for the development environment, and assess the effectiveness of software security.
Course Agenda

Domain 1: Security and Risk Management

Domain 2: Asset Security
Domain 3: Security Architecture and Engineering
Domain 4: Communication and Network Security
Domain 5: Identity and Access Management (IAM)
Domain 6: Security Assessment and Testing
Domain 7: Security Operations
Domain 8: Software Development Security

Domain 1: Security and Risk Management

Overview

Domain 1 of the (ISC)² CBK lays the foundation for the entire course, introducing concepts and principles that will be utilized throughout. It is imperative that the candidate learn and understand these thoroughly, if the candidate is not already familiar with the material from professional practice.

NOTE: Throughout this domain and much of the rest of the course material, the term “organization” will be used to describe operational entities; an organization might be a private business operating in a market dynamic, a government entity, or a nonprofit/charitable agency of some kind. This term is used in generic fashion as a consideration that candidates may work for any type of functional unit; the material is designed to be agnostic to the type of industry or nature of work a particular unit might be involved in. When material is specific to a certain type of organization, it will be specified in context (for instance, a bank as a financial organization has specific security concerns not faced by other types of organizations).
Domain Objectives

After completing this domain, the participant will be able to:

1. Explain the concepts of confidentiality, integrity, and availability.
2. Differentiate between confidentiality, integrity, and availability.
3. Recognize security governance principles.
4. Describe how the security function of an organization aligns to that organization’s business strategy, goals, mission, and objectives.
5. Describe various typical roles and responsibilities related to security within organizations.
6. Identify governance processes within organizations, and explain how those may affect security.
7. Identify specific security control frameworks based on a brief description or list of framework attributes.
8. Discern between the concepts and meaning of “due care” and “due diligence.”
9. Describe common practices used for asset valuation and the challenges/benefits associated with each.
10. Distinguish between threats and vulnerabilities.
11. Identify common practices of risk assessment and analysis.
12. Know the four common methods of risk management.
13. Know how to choose from the four common methods of risk management.
14. Recognize common practices for selecting security controls.
15. List the various types, classes, and categories of security controls.
16. Describe the importance of monitoring and measuring the security program and controls and why this is performed on a continuous basis.
17. Recognize common risk frameworks.
18. Apply risk-based management concepts to the supply chain and the use of third parties for risk assessment and monitoring.
20. Apply threat modeling methodologies.
22. Recognize the purpose of the service level agreement, how it augments the contract, and which items should be contained in each.
23. Determine and document minimum security requirements.
24. Recognize the various forms of compliance requirements (laws/regulations, standards, and contracts).
25. Understand the concept of regulatory compliance, especially in the context of modern privacy requirements, and identify typical regulations encountered in practice.
27. Recognize modern international legal restrictions on import/export of data and IT tools.
28. Identify common privacy terms used in current personal data protection laws worldwide.
29. Describe the hierarchy of written governance (policies, standards, guidelines, and processes).
30. Identify the various means to support personnel security goals, including common policies and procedures.
31. Explain how modern legal frameworks affect international data flow and how the information security industry is responsible for many compliance requirements.
32. Describe the importance of security training, education, and awareness and how to differentiate between those elements.
33. Describe the necessity of business continuity and disaster recovery (BCDR) functions, and recognize basic foundational concepts.
34. Explain the ethical standards to which a professional security practitioner will be expected to uphold, as well as the standards of behavior and performance expected of (ISC)² members.
## Domain Agenda

<table>
<thead>
<tr>
<th>Module</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Concepts of Confidentiality, Integrity, and Availability</td>
</tr>
<tr>
<td>2</td>
<td>Organizational/Corporate Governance</td>
</tr>
<tr>
<td>3</td>
<td>Risk Management Concepts</td>
</tr>
<tr>
<td>4</td>
<td>Compliance Requirements</td>
</tr>
<tr>
<td>5</td>
<td>Legal and Regulatory Issues that Pertain to Information Security in a Global Context</td>
</tr>
<tr>
<td>6</td>
<td>Security Policy, Standards, Procedures, and Guidelines</td>
</tr>
<tr>
<td>7</td>
<td>Personnel Security Policies and Procedures</td>
</tr>
<tr>
<td>8</td>
<td>Security Awareness, Education, and Training Program</td>
</tr>
<tr>
<td>9</td>
<td>Business Continuity Requirements</td>
</tr>
<tr>
<td>10</td>
<td>Professional Ethics</td>
</tr>
<tr>
<td>11</td>
<td>Domain Review</td>
</tr>
</tbody>
</table>
Module 1: Concepts of Confidentiality, Integrity, and Availability

Module Objectives
1. Explain the concepts of confidentiality, integrity, and availability.
2. Differentiate between confidentiality, integrity, and availability.
Confidentiality, Integrity, and Availability (CIA) Triad

When practitioners discuss the field of security, we concentrate on three goals: ensuring the confidentiality, integrity, and availability (CIA) of assets. This is referred to as the CIA triad. In information security, the assets are data—information that requires security. This is true for data in any form, whether it is stored electronically or in printed hardcopy, and it also applies to any systems/mechanisms/techniques used to process/manipulate/store that data.

Explaining the CIA triad in more detail, in the context of information security:

**Confidentiality:** only authorized entities have access to the data.

**Integrity:** there are no unauthorized modifications of the data.

**Availability:** authorized entities can access the data when and how they are permitted to do so.

CIA Triad Examples:

A lock on a file cabinet can provide confidentiality; only authorized personnel will be given a key to access the information inside the cabinet.

Using a template for version control of a document; comparing copies of the document against the template ensures the integrity of the data in the copies.

A backup of data stored electronically ensures availability of the data; if the primary version of the data is rendered useless, a copy of the backup can be restored and used as the new primary.

Some security controls provide other functions that are not aspects of the triad but are also desirable. These include nonrepudiation and authentication, which will be discussed in a subsequent domain.

The CIA triad is a fundamental concept of our field and is absolutely essential to understand. A lot of the material discussed throughout the course will be couched in its relation to the triad.
Module Objectives

1. Recognize security governance principles.
2. Describe how the security function of an organization aligns to that organization’s business strategy, goals, mission, and objectives.
3. Describe various typical roles and responsibilities related to security within organizations.
4. Identify governance processes within organizations and how those may affect security.
5. Identify specific security control frameworks based on a brief description or list of framework attributes.
6. Discern between the concepts and meaning of “due care” and “due diligence.”
Security Governance Principles

Governance is the process of how an organization is managed. This includes all aspects of how decisions are made for that organization, and can (and usually does) include the policy, roles, and procedures the organization uses to make those decisions.

Security governance, then, is the entirety of the policies, roles, and processes the organization uses to make security decisions. Just as each organization has its own unique governance structure, it will also have security governance specific to its purposes and objectives.

Aligning the Security Function to the Organization’s Business Strategy, Goals, Mission, and Objectives

It is absolutely imperative that security not operate in a way that is exclusive to and ignorant of the overall purpose and objective of the organization. In most cases, security is a support function; that is to say, the business could exist without the security department, but the security department could not exist without the business.

Note: The exception to this, of course, is organizations that provide security products/services; in those organizations, security is a core component of operations, and the organization could not exist without security.

Therefore, the security practitioner must understand how the organization functions and what its goals are, then determine how security can best enhance those functions and the attainment of those goals. Security governance that does not align properly with organizational goals can lead to implementation of security policies and decisions that unnecessarily inhibit productivity, impose undue costs, and hinder strategic intent.

Organizational Processes

As mentioned earlier, one significant aspect of governance is the process of how a decision is made within an organization. This can be accomplished in a number of ways, according to a variety of factors. For instance, a small private business might have a very simplistic process for making decisions: the small business owner makes every decision based on their own judgment and the information they have available. A corporation, on the other hand, might have a decision-making process that is dictated by several sources: the government body where the company is chartered might have legislation regarding how corporations must make strategic decisions and which policies are required of all corporations; the board of directors might impose a corporate mandate.
for particular types of decisions (which might require including the board, as one step in the process); local and federal regulators might dictate who within the corporation participates and finalizes particular decisions, and so on.

Each organization will have its own process for making decisions, based on its structure, goals, nature, and industry. Some companies make use of a governance committee; a formal body of personnel who determine how decisions will be made within the organization and the entity that can approve changes and exceptions to current relevant governance. Governance committees are required for most nonprofit organizations; the governance committee recruits and selects board members and determines if the board as a whole (and individual members) are performing optimally.

Just as security decisions can affect the overall business goals of the organization, organizational decisions can affect security. Following are some business decisions that might affect the organization’s security:

- **Acquisition**: If the organization decides to purchase another business unit to have as a subsidiary, the security implications are extensive. If there is a significant difference in security policies and practices between the entities, the security professionals in both groups will have to decide how best to align the two, with guidance and final decision from senior management.

- **Merger**: Much like an acquisition, a merger of two organizations entails aligning the security governance of the resulting entity.

- **Divestiture**: If an organization decides to sell off or cede control of a subsidiary, a considerable amount of effort will have to go into determining which of the resulting entities controls proprietary property, to include data, which may entail a great deal of effort on the part of the security personnel.

In each of these examples, external entities, such as regulators and investors, may have additional input and control in determining the outcome. These examples are not exhaustive; many organizational decisions will have vast security ramifications.

**Organizational Roles and Responsibilities**

An organization’s hierarchy is often determined by the goals of the organization or which industry it operates in. This structure can
have a bearing on how security governance is created and implemented, or even how security functions are performed.

The following are a sampling of various roles pertaining to security encountered in many organizations. This list is in no way inclusive of all types of organizational structures and is not presented as a definitive guide to these roles; it is simply a way to demonstrate the form of some organizations and the bearing of some roles on organizational security.

- **Senior management:** The upper strata of the organization, comprising those officers and executives that have the authority to obligate the organization and to dictate policy. These can include such roles as president, vice president, chief executive officer (CEO), chief operating officer (COO), chief information officer (CIO), chief security officer (CSO), chief financial officer (CFO), and the like. Usually, these roles include personnel with some direct legal or financial responsibilities according to statute or regulation. Senior management is typically responsible for mandating policy, determining the strategic goals for the organization, and making final determinations according to the organizational governance for both security and non-security topics.

- **Security manager/security officer/security director:** Often, this is the senior security person within an organization. In some cases, the organization has a CSO (mentioned in the preceding entry of this list), in which case the security officer is a member of senior management. When the senior security role is not a member of senior management, the reporting hierarchy is an essential element of determining the importance and influence security has within the organization. For instance, an organization wherein the security manager reports directly to the CEO places a great deal of importance on security; an organization that has the security manager reporting to an administrative director, who in turn reports to a vice president, who reports to senior management, obviously does not. The security manager is typically responsible for advising senior management on security matters, may assist in drafting security policy, manages day-to-day security operations, represents the organization’s security needs in groups and meetings such as the Configuration Management Board and similar committees, contracts for and selects security products and solutions, and may manage the organization’s response to incidents and disasters.

  **Note:** According to industry best practices, the security manager should not report to the same role/department that is in charge of information technology (IT) because the functions are somewhat
adversarial (the security team will be reporting on/reviewing the operations and productivity of the IT team). Having the same department responsible for both functions would constitute a form of conflict of interest. The exception to this is when both the security office and the IT department report to the chief information officer (CIO); this is usually an acceptable form of hierarchy.

- **Security personnel**: The security practitioners within the organization. These can include administrators, analysts, incident responders, and so forth. This group may also include personnel from disciplines other than IT security, such as physical security and personnel security. Security personnel are tasked with performing the security processes and activities within the organization. Security personnel usually report to the security manager/director/officer.

- **Administrators/technicians**: IT personnel who regularly perform work within the environment may have security duties as well. These can include secure configuration of systems, applying secure networking, reporting potential incidents, and so forth. Positions in this category include but are not limited to: system administrators (often Tech Support and Help Desk personnel) and network administrators/engineers. This group typically reports to the IT director or CIO.

- **Users**: Employees, contractors, and other personnel who operate within the IT environment on a regular basis. While this role does not have specific security duties per se, users are required to operate the systems in a secure fashion, and they are usually required to sign a formal agreement to comply with security guidance. Users may also be co-opted and trained to report potential security incidents, acting as a rudimentary form of intrusion detection. Users typically report to their functional managers.

**Security Control Frameworks**

In formalizing its security governance, an organization might implement a **security control framework**; this is a notional construct outlining the organization’s approach to security, including a list of specific security processes, procedures, and solutions used by the organization. The framework is often used by the organization to describe its security efforts, for both internal tracking purposes and for demonstration to external entities such as regulators and auditors.
There are a variety of security frameworks currently popular in the industry, each offering benefits and capabilities, usually designed for a certain industry, type of organization, or approach to security. The following list of framework examples is by no means exhaustive or intended to be exclusive; the security practitioner should have a working familiarity with the frameworks on this list, as well as whatever framework is used by their own organization (if any). Some of these frameworks will be discussed in more detail later in the course.

- **ISO 27001/27002**: The International Standards Organization (ISO) is recognized globally, and it is probably the most pervasive and used source of security standards outside the United States (American organizations often use standards from other sources). ISO 27001 is known as the information security management system (ISMS) and is a comprehensive, holistic view of security governance within an organization, mostly focused on policy. ISO 27002 is a comprehensive list of security controls that can be applied to an organization; the organization uses ISO 27002 to select the controls appropriate to its own ISMS, which the organization designs according to ISO 27001. ISO standards are notably thorough, well-recognized in the industry, and expensive relative to other standards. Use of ISO standards can allow an organization to seek and acquire specific standards-based certification from authorized auditors.

- **COBIT**: Created and maintained by ISACA, the COBIT framework (currently COBIT 5) is designed as a way to manage and document enterprise IT and IT security functions for an organization. COBIT widely uses a governance and process perspective for resource management and is intended to address IT performance, security operations, risk management, and regulatory compliance.

- **ITIL**: An IT service delivery set of best practices managed by Axelos, a joint venture between the British government and a private firm. ITIL (formerly the Information Technology Infrastructure Library, now simply the proper name of the framework) concentrates on how an organization’s IT environment should enhance and benefit its business goals. ITIL is also mapped to the ISO 20000 standard, perhaps the only non-ISO standard to have this distinction. This framework also offers the possibility for certification, for organizations that find certification useful.

- **RMF**: NIST, the U.S. National Institute of Standards and Technology, publishes two methods that work in concert (similar to how ISO 27001 and 27002 function); the Risk Management
Framework (RMF), and the applicable list of security and privacy controls that goes along with it (respectively, these documents are Special Publications (SPs) 800-37 and 800-53). While the NIST SP series is only required to be followed by federal agencies in the United States, it can easily be applied to any kind of organization as the methods and concepts are universal. Also, like all American government documents, it is in the public domain; private organizations do not have to pay to adopt and use this framework. However, there is no private certification for the NIST framework.

- **CSA STAR**: The Cloud Security Alliance (CSA) is a volunteer organization with participant members from both public and private sectors, concentrating—as the name suggests—on security aspects of cloud computing. The CSA publishes standards and tools for industry and practitioners, at no charge. The CSA also hosts the Security, Trust, and Assurance Registry (STAR), which is a voluntary list of all cloud service providers who comply with the STAR program framework and agree to publish documentation on the STAR website attesting to compliance. Customers and potential customers can review and consider cloud vendors at no cost by accessing the STAR website. The STAR framework is a composite of various standards, regulations, and statutory requirements from around the world, covering a variety of subjects related to IT and data security; entities that choose to subscribe to the STAR program are required to complete and publish a questionnaire (the Consensus Assessments Initiative Questionnaire (CAIQ), colloquially pronounced “cake”) published by CSA. The STAR program has three tiers, 1–3, in ascending order of complexity. Tier 1 only requires the vendor self-assessment, using the CAIQ. Tier 2 is an assessment of the organization by an external auditor certified by CSA to perform CAIQ audits. Tier 3 is in draft form as of the time of publication of this CBK; it will require continuous monitoring of the target organization by independent, certified entities.

**Due Care/Due Diligence**

**Due care** is a legal concept pertaining to the duty owed by a provider to a customer. In essence, a vendor has to engage in a reasonable manner so as not to endanger the customer: the vendor’s products/services should deliver what the customer expects, without putting the customer at risk of undue harm.
An example to clarify the concept: if a customer buys a car from the vendor, the vendor should have designed and constructed the car in a way so that the car can be operated in a normal, expected manner without some defect harming the customer. If the user is driving the car normally on a road and a wheel falls off, the vendor may be culpable for any resulting injuries or damage if the loss of the wheel is found to be the result of insufficient care on the part of the vendor (if, say, the wheel mount was poorly designed, or the bolts holding the wheel were made from a material of insufficient strength, or the workers assembling the car did so in a careless or negligent way). This duty is only required for reasonable situations; if, for instance, the customer purposefully drove the car into a body of water, the vendor does not owe the customer any assurance that the car would protect the customer, or even that the car would function properly in that circumstance.

NOTE: There is a joke regarding the standard of reasonableness that lawyers use—“Who is a reasonable person? The court. The court is a reasonable person.” Meaning that the “standard” is actually quite ambiguous and arbitrary: the outcome of a case hinging on a determination of “reasonable” action is wholly dependent on a specific judge on a specific day, and judges are only people with opinions.

**Due diligence**, then, is any activity used to demonstrate or provide due care. Using the previous example, the car vendor might engage in due diligence activities such as quality control testing (sampling cars that come off the production line for construction/assembly defects), subjecting itself to external safety audit, prototype and regular safety testing of its vehicles to include crash testing, using only licensed and trained engineers to design their products, and so forth. All of these actions, and documentation of these actions, can be used to demonstrate that the vendor provided due care by performing due diligence.

In the IT and IT security arena, due diligence can also take the form of reviewing vendors and suppliers for adequate provision of security measures; for instance, before an organization uses an offsite storage vendor, the organization should review the vendor’s security governance, and perhaps even perform a security audit of the vendor to ensure that the security provided by the vendor is at least equivalent to the security the organization itself provides to its own customers. Another form of due diligence for security purposes could be proper review of personnel before granting them access to the organization’s data, or even before hiring; this might include background checks and personnel assurance activities. (Personnel security measures, which provide a measure of due diligence, will be discussed in more detail later in this domain.)
NOTE: In recent years, regulators and courts (both of which are often tasked with determining sufficient provision of due care) have found certain activities to be insufficient for the purpose of ensuring due diligence, even though those activities were previously sufficient. Specifically, publishing a policy is an insufficient form of due diligence; to meet the legal duty, an organization must also have a documented monitoring and enforcement capability in place and active to ensure the organization is adhering to the policy.
Module 3: Risk Management Concepts

Module Objectives

1. Describe common practices used for asset valuation and the challenges/benefits associated with each.
2. Distinguish between threats and vulnerabilities.
3. Identify common practices of risk assessment and analysis.
4. Know the four common methods of risk management.
5. Know how to choose from the four common methods of risk management.
6. Recognize common practices for selecting security controls.
7. List the various types, classes, and categories of security controls.
8. Describe the importance of monitoring and measuring the security program and controls and why this is performed on a continuous basis.
9. Recognize common risk frameworks.
10. Apply risk-based management concepts to the supply chain and the use of third parties for risk assessment and monitoring.
11. Recognize standard threat modeling concepts.
12. Apply threat modeling methodologies.
13. Recognize common threats and risks.
14. Recognize the purpose of the service level agreement, how it augments the contract, and which items should be contained in each.
15. Determine and document minimum security requirements.
Risk Management Concepts

Risk is the possibility of damage or harm and the likelihood that damage or harm will be realized. The security practitioner’s job is to manage risk for the organization, according to the organization’s strategy and needs. The senior management of the organization will determine what level of risk (and if a particular risk) is suitable relative to the rewards offered by conducting operations; this is known as acceptable risk. Every organization makes its own determination of what constitutes acceptable risk and how to manage risk.

Asset Valuation

To effectively manage risk, the organization must determine what assets it has and assign a value to those assets. Assets can include property (both tangible and intangible), people, and processes.

NOTE: In modern organizations, data (an intangible asset) is often the property with the most significant particular value.

An asset inventory is crucial for this task; it is impossible to protect what you have if you don’t know what you have. There are many tools to aid in an asset inventory, automated and otherwise. It is important for the organization to mesh its acquisition and development processes with the asset inventory method it uses so that all new assets will be included in the inventory.

There are many ways to determine the value of an asset. An asset might have a discrete market value (a monetary value). Conversely, an asset might have a particular relative value for the organization; a specific asset that might otherwise be of nominal value to another organization might have great importance to your organization. It is important for senior management to review and oversee asset value determinations so that your organization is properly assigning value to its assets.

However, while senior management will make the final determination of value for the organization’s assets, the main effort of valuation will fall to the functional managers. Usually, it is the line managers who will have the best perspective of the assets under their control, because they will be the people working with those assets the most; they will have the greatest insight and understanding of how those assets are used by the organization.

NOTE: It is important to remember when gathering asset valuation information that while unit managers will have the best insight to the value of the assets under their control, managers are also inherently biased. When asked, “what assets are most important to
the organization,” the response is almost invariably, “mine.” This is not a result of malicious intent, it is simply human nature. Therefore, senior management must bear this phenomenon in mind while reviewing the valuation survey information and adjust for any possible overvaluation that may have occurred.

One tool used widely in the industry is the **business impact analysis (BIA)**. The BIA is a list of the organization’s assets, annotated to reflect the criticality of each asset to the organization. Because each organization operates differently, assets that are critical to one organization might have little relative importance to other organizations, even within the same field or industry. The personnel involved in creating the organization’s BIA will need to understand not only the nominal value of each asset itself, but the business functions and operations of the organization so as to properly determine that asset’s criticality. The use of the BIA will transcend asset valuation, and the BIA can be used in other components of risk management as well as other aspects of security.

**Identify Threats and Vulnerabilities**

The next step in the risk management process is to identify threats and vulnerabilities associated with the organization’s assets. **Threats** are any aspects that create a risk to the organization, its function, and its assets. **Vulnerabilities** are any aspects of the organization’s operation that could enhance a risk or the possibility of a risk being realized.

Threats can take many forms, anthropogenic and otherwise, and can be the result of no motivation, malicious intent, or inadvertent action. Consider the following list of common threats and the brief description of each:

- **Natural**: Nature has no malicious intent; it does not have any desire to interrupt business operations or to harm people. It is, however, a threat to both operations and health and human safety. Natural phenomena that fall into this category include disasters (floods, hurricanes, earthquakes, and so on), fire (on a disaster scale, or localized), and biologics. The latter category includes such things as small animals affecting operations by chewing through conduit/cables, which has caused both widespread and localized outages, for both power and data connectivity; that category can also include pandemic disease, which can interrupt operations significantly.

- **Criminal activity**: People with specific intent to do harm by performing illegal activity; the intended harm can be financial or physical. Hackers, thieves, espionage agents, social activists, and...
terrorists all fall into this category. This sort of activity can come from external sources, or personnel internal to the organization.

- **User error**: Users can conduct a vast variety of inadvertent activity that can affect all aspects of the CIA triad. These include actions as simple as spilling coffee, tripping over a cable, deleting a certain file unintentionally, or releasing confidential information accidentally.

**NOTE**: This is a far from comprehensive list of threats, and is only meant as an introduction to the concept.

There are many ways to categorize and tabulate threats; there is no one way that is correct for every organization. More importantly, every organization will face threats particular to its own industry, market, location, and type of operation. Threats also fluctuate continually; there is no static threat landscape because both the organization and the world it operates in continue to evolve.

The security practitioner, on behalf of the organization, must constantly assess this evolving threat picture. It is important to stay current with evolving threats by monitoring global, national, and local news, organizational operations, and the activity of those entities that might pose threats to the organization. In addition to organizational efforts, there are vendors that supply threat intelligence information on a contract basis, predicting potential new (and increased existing) threats and notifying their customers.

The organization must also assess and inventory existing and potential vulnerabilities. In any situation where a threat could exploit a means to cause harm to the organization and/or its assets, a vulnerability exists.

There are many tools and methods for discovering and tabulating vulnerabilities, both manually and with automation.

A small sampling of types of vulnerabilities:

- **Software**: There are many examples of software functions that allow an attacker to affect some aspect of the CIA triad; these software functions might be defects in the original programming, or intentional programmatic elements that can be utilized maliciously for outcomes unintended by the vendor/owner of that software.

- **Physical**: Any aspect of the physical facilities or operations of an organization that may pose danger to the organization
or its personnel could be considered a vulnerability. Vulnerabilities might include the entrances to the facility, flammable locations/items, easily portable assets, and sometimes even line of sight.

- **Personnel**: The organization’s own personnel might be vulnerable to attack either physically or by means of subversion/persuasion. The personnel might also pose a vulnerability, themselves as internal threats with access to the organization and its operations.

**NOTE**: This is a far from comprehensive list of vulnerabilities, and is only meant as an introduction to the concept.

### Risk Assessment/Analysis

After the organization has conducted a thorough asset inventory and valuation and identified the threats and vulnerabilities the organization is subject to, it is possible for the organization to realistically assess risk.

Because risk (as defined earlier in this domain) involves the likelihood a risk will be realized, in addition to identifying possible types of damage/harm, it is important that professionals tasked with performing risk analysis also be able to gather information from sources external to the organization to accurately gauge the potential of occurrence.

Risk can generally be rated according to three factors: impact, likelihood, and exposure.

**Impact**: The damage/harm caused if the risk is realized. This can be measured monetarily as an effect to health and human safety, and/or the criticality of the affected asset to the organization. The BIA, mentioned earlier in this domain, is an excellent tool for use in this aspect of risk assessment.

**Likelihood**: A measure of the possibility the risk will be realized. This can be extremely difficult to determine as it is a form of prediction. Often, this determination is aided by the use of historical data from both within and external to the organization (answering the questions: “how often does this happen to us? how often does it happen, in general?”).

**Exposure**: Establishing the realistic potential for the organization to face certain types of threats. Obviously, the organization will have a greater exposure to those threats posed by the organization’s activities (for instance, an organization involved in commercial fishing faces the threat of losing personnel to drowning, whereas a metropolitan bicycle messenger service does not). Location might be another factor that affects exposure; some natural disasters are native to certain geographic locations, while others are not.
It is essential to remember that there is no such thing as “zero risk”—all activities entail some element of risk, and all threats have a potential, even if miniscule or highly unlikely, for occurrence.

Risk analysis is typically split into two categories: qualitative and quantitative. These are somewhat academic distinctions, but the candidate should understand them for purposes of adhering to the CBK.

- **Qualitative:** A subjective approach to risk analysis. The organization should opt for this method when the organization does not have a sufficient availability of time, budget, or personnel trained in risk analysis to put toward the effort.

- **Quantitative:** An objective approach to risk analysis; the quantitative method should produce objective, discrete numeric values. The organization should opt for this method when it has sufficient time, budget, and personnel trained in risk analysis to put toward the effort.

Both methods require personnel who are familiar with the organization’s operation, relevant threats, assets, and vulnerabilities.

**Risk Response**

Figure 1.1 shows the four general methods an organization can use to address risk.

---

**General Risk Management Options**

![Diagram of General Risk Management Options]

*Figure 1.1: General Risk Management Options (go-by)*
**Risk avoidance** is a business decision, not a security practice. Senior management may choose risk avoidance when the potential impact of a given risk is too high to be reasonably offset by the potential rewards of the business function, or if the likelihood of the risk being realized is simply too great.

**Risk acceptance** is the converse of avoidance; management may opt for conducting the business function that is associated with the risk without any further action on the part of the organization, either because the impact or likelihood of occurrence is negligible, or because the benefit is more than enough to offset that risk.

**Risk mitigation** is the realm of the security practitioner; in risk mitigation, **security controls** are applied to the operational element that is susceptible to (or causing) the risk to reduce either the impact or the likelihood (or both) of the risk being realized.

**Risk transference** is the practice of paying another party to accept the full financial impact of the harm resulting from a risk being realized, in exchange for payment of a fractional amount of the full impact cost. Typically, this is an insurance policy with premiums adjusted for a number of factors (the potential likelihood and impact, the use of security controls, frequency of payments, etc.).

**Activity: Swimming with Sharks**

The organization must determine how to address risks associated with each new operational function. This activity allows the candidate to demonstrate understanding of the common approaches to risk management.

You are the security manager for a commercial fishing operation. Your company is considering adding a new line of business to the organization in the form of ecotourism, where paying customers join your crews at work sites and are lowered into the water in steel cages to observe and photograph sharks.

Senior management is considering the different risk management approaches for handling the risks inherent to this new line of business.

**Instructions**
Working as a group and using this scenario, describe each of the four approaches to risk management in the context of the example. For the mitigation portion, brainstorm a brief list of security controls that might be included. You have 10 minutes.
Whenever risk mitigation is performed, there will always be some degree of risk that remains after the security controls are put into place: there is no such thing as either zero risk or 100 percent security. We call this remaining risk “residual risk.” The goal of risk mitigation is to reduce the residual risk down to a level of acceptable risk and then to accept that remaining risk. Therefore, whenever an organization engages in risk mitigation, it must also perform risk acceptance at some point.

Security Controls

Security controls are methods, tools, mechanisms, and processes used in risk mitigation. Security controls can function in two general ways: as safeguards, which reduce risk impact/likelihood before the realization of the risk has occurred, and countermeasures, which reduce the impact/likelihood afterwards.

For example, a wall could be a safeguard, preventing hostile people from entering the facility, while a motion sensor could be considered a countermeasure as it sends an alert when someone has entered the area in an unauthorized fashion.

Security controls should be chosen according to a cost/benefit analysis, comparing the expense of acquiring, deploying, and maintaining the control against the control’s ability to reduce the impact/likelihood of a specific risk (or set of risks). It is also crucial to weigh the operational impact that will be caused by the control itself against the benefit of continuing that business function with the risk reduction offered by that control.

NOTE: It is essential to remember that every security control has an attendant negative impact on operations, whether that is a monetary cost or a reduction in user capability or convenience; there is always a tradeoff between security and productivity that makes the security team and the operations group somewhat adversarial in many organizations. The security practitioner is tasked with aiding the organization to find the right balance. As Dr. Eugene “Spaf” Spafford of Purdue University once put it: “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then, I have my doubts.”
http://spaf.cerias.purdue.edu/quotes.html
Traditional Model

One traditional method for selecting the appropriate security controls has been the use of the “loss expectancy” model:

annual loss expectancy (ALE) = single loss expectancy (SLE) x annual rate of occurrence (ARO)

In detail, it works like this:

The SLE is the expected negative impact related to a particular risk (the risk being assessed). Most often, this is expressed monetarily. It is calculated by determining the value of the asset that might be affected (or lost) and multiplying it by an “exposure factor”—a percentage that represents the amount of damage resulting from that type of loss.

So:

SLE = asset value (AV) x exposure factor (EF)

The ARO is the number of times per year a given impact is expected, expressed as a number.

So, the ALE is the SLE multiplied by the ARO, which gives us the estimated annual cost related to a particular risk.

The value of the ALE to the organization is that it allows the organization to determine whether the cost of a particular kind of control for a specific risk is worth the investment.

Let’s use an example to demonstrate:

You are the security manager of a retail store located in a shopping mall. Senior management has tasked you with reviewing the options for managing the risk associated with shoplifting.

To approach this decision, you first determine the SLE: what the loss is to the company in a single event of shoplifting. Several factors go into this determination. For instance, the size of the items you sell: it is easier to shoplift small personal electronic devices than it is to shoplift, say, major appliances such as washing machines; this is how you determine the exposure factor. You also need to know the value of the assets that might be subject to shoplifting: what is the value to your company, of any one item in the inventory you sell? What is the wholesale value? What is the retail value? Which have you lost if that item is stolen?

Let’s say you determine that based on the items you have for sale, a single loss expectancy for shoplifting, on average, is $5. You then have to determine the ARO.
How is this done; how do you predict how many shoplifting events will occur at your store in a year? Well, this data is already available; major insurers and retail trade groups have historical data about shoplifting gathered over many decades of retail sales, insurance claims, and police reports of theft. In fact, there are historical retail data sets that are so specific, the data can predict the ARO of shoplifting based on your retail location, the physical footprint (size) of your store, and the inventory you carry. While historical data used to predict future activity are not perfect (financial markets crash on a fairly regular basis, and vast, detailed financial data exists and does not seem to obviate this activity), they can, on average, be useful for making this kind of assessment.

So, for purposes of this example, let’s say you determine that your store can expect 1,000 shoplifting events in the course of a year. This is your ARO for shoplifting.

With the ARO and SLE, you can easily determine the ALE: $5 \times 1,000 = $5,000

You know that shoplifting will, on average, cost your company $5,000 per year. Using this figure, you can assess various risk management options for addressing shoplifting. For instance, hiring a security guard might cost the company $50,000 per year. Compared to the risk (the ALE), this seems extremely disproportionate: even if the guard prevents all shoplifting attempts, your company would be losing $45,000 more than if you did nothing at all. You might also look at other options: hardware tethers/locks for display merchandise, video surveillance, radio-frequency identification (RFID) alarm chips, and so forth. For each type of security control to address shoplifting, you can compare the cost to the ALE. Remember that the cost of the control includes more than the acquisition price: it also includes the costs of annual maintenance and operation of that control. Let’s say, in this demonstration case, the most cost-effective control you can find to attenuate the possibility and effects of shoplifting will cost the company $15,000 per year.

For our example, security controls (a form of risk mitigation) are not the only option: you might consider risk transference, as well. This would entail getting a quote from an insurance company for a shoplifting policy. For example purposes, let’s say you receive a number of quotes, and the lowest price of an annual policy is $10,000.

So, let’s review the risk management options using this example data from the ALE:

**Risk mitigation:** The ALE is $5,000 and the most reasonable control is $15,000; risk mitigation is not a rational option.
Risk transference: The ALE is $5,000 and the cost of transferring is $10,000; risk transference is not a rational option.

Risk avoidance: If the company did not offer merchandise for sale, it would no longer be a retail sales operation; risk avoidance, in this case, does not make much sense.

Risk acceptance: Because the other options do not make sense from a financial standpoint, and because the company wants to remain a retail operation, the company could reasonably accept the risk due to shoplifting.

NOTE: The ALE is a rudimentary and mature model, inherited from the realm of physical security, and is well suited to examples of this kind. It is not particularly apt for IT security: in our field, there is no good way to assess SLE; a loss event is rarely nominal, moreover, we are typically not allowed to have an ARO other than 1—whenever a vulnerability is discovered because a loss has been realized, we are required to take steps to remediate that vulnerability so that specific type of loss should not be repeated. An organization that has repeated, continuous losses related to data/IT will soon be beleaguered by regulators, service providers, and customers alike. So, this model doesn’t work well for IT security. However, it is still used throughout the industry and is an aspect of security that the candidate is required to understand as part of the CBK.

Applicable Types of Controls

Security controls can be arranged according to many criteria. One way to consider controls is by the way the controls are implemented.

Technical/logical controls: Controls implemented with or by automated or electronic systems. Examples include firewalls, electronic badge readers, access control lists, and so on. Many IT systems include some kind of technical control capacity or functionality; for instance, routers can be set to reject traffic that may be indicative of possible attacks.

Physical controls: Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, and so forth. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

Administrative controls: Controls implemented through policy and procedure. Examples include access control processes and requiring multiple personnel to conduct a specific operation. Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager.
Security Control Categories

Another way to group security controls is by how they take effect. In the security industry, controls are typically arranged into these categories:

**Directive:** Controls that impose mandates or requirements. These can include policies, standards, signage, or notification, and are often combined with training.

**Deterrent:** Controls that reduce the likelihood someone will choose to perform a certain activity. These can include notification, signage, cameras, and the noticeable presence of other controls.

**Preventative:** Controls that prohibit a certain activity. These can include walls and fences; they prohibit people from entering an area in an unauthorized manner.

**Compensating:** Controls that mitigate the effects or risks of the loss of primary controls. Examples include physical locks that still function if an electronic access control system loses power, or personnel trained to use fire extinguishers/hoses in the event a sprinkler system does not activate.

**Detective:** Controls that recognize hostile or anomalous activity. These can include motion sensors, guards, dogs, and intrusion detection systems.

**Corrective:** Controls that react to a situation in order to perform remediation or restoration. Examples include fire suppression systems, intrusion prevention systems, and incident response teams.

**Recovery:** Controls designed to restore operations to a known good condition following a security incident. These can include backups and disaster recovery plans.

This form of categorization is not absolute or distinct; many controls can fall into several categories, depending on their implementation and operation. For instance, surveillance cameras can control that are deterrent (just the presence of cameras discourages someone from entering a surveilled area, for fear of being observed), detective (when combined with live monitoring by guards or a motion-sensing capability), and compensating (when providing additional detection capability that augments gate guards or other controls). Controls of the various types (administrative, technical, and physical) can be used in each of the categories.
When selecting and implementing security controls, it is always preferable to use multiple types and implement them among the various categories than to rely on one type or category; this is called defense in depth (also known as layered defense), where controls of various types and kinds overlap each other in coverage. There are two reasons to implement defense in depth:

- Relying on a single control type or category increases the possibility that a single control failure could lead to enhanced risk. For instance, if the organization were to rely solely on technical controls and power was interrupted, those controls would not function properly. Moreover, a new vulnerability might be discovered in a specific control; if that was the sole control your organization relied on, your organization would become completely exposed.

- Using multiple types and categories of controls forces the aggressor to prepare multiple means of attack instead of just one. By making the task of the attacker more complicated, we reduce the number of possible attackers (many people know one thing well, but few people know many things well). For instance, combining strong technical and physical controls could require the aggressor to have both hacking and physical intrusion toolkits, which increases the price of the attack for attacker, thereby reducing the number of potential attackers.

Monitoring and Measurement

Implementation of security controls is not the final action necessary for risk mitigation; the security professional must monitor the function and operation of security controls for the organization to determine if they are performing correctly and that they continue to provide the risk coverage as intended.

Often referred to as a security control assessment (SCA) a plan and process for determining the proper function and management of controls is necessary and should be customized to the needs of the organization. This is very similar to an audit with specific focus on security controls and includes performance of those controls.

The security team is often tasked with assembling SCA data and presenting a report to senior management, detailing which controls are not performing as expected and which risks are not being addressed by the current control set. This information might be gathered by the security team itself through the use of automated monitoring tools, or it might be delivered by internal sources (such as the IT department) as part of a self-reporting mechanism, or from external sources (such as a third-party
security monitoring vendor). The security practitioner must collect all relevant data and distill it into a form that is understandable and useful to management.

This security control monitoring effort should not be a singular event or even a recurring task; the industry standard for security control maintenance and improvement is a continual, ongoing, enduring activity. Threats continue to evolve, the organization’s IT environment is continually being updated and modified, and security tools continue to improve; these situations require constant action on the part of security practitioners.

Other control assessment techniques include vulnerability assessments and penetration tests:

- **Vulnerability assessment:** Often performed with automated tools, the vulnerability assessment reviews the organization’s IT environment for known vulnerabilities, cataloging and often sending alerts for any detections. NOTE: vulnerability assessments are often limited in the respect that they only detect known vulnerabilities; relying wholly on vulnerability assessments to determine the organization’s risk profile is inadequate, because there may exist vulnerabilities that have not yet been discovered and are not in the signature database of the assessment tool.

- **Penetration test:** A trusted party (internal or external to the organization) tries to gain access to the organization’s protected environment to simulate an external attack and test the organization’s security defenses. There are many ways to structure a penetration test, including requiring that the adversarial parties (the organization’s security team and the penetration testers) have no knowledge beyond what an attacker would have: the security team is not given forewarning that the test is taking place, and the testers are not given details about the organization’s environment or security. Ethical penetration testing requires that any test not create a risk to health and human safety or destroy property. It is essential to properly coordinate any penetration test before the engagement to stipulate any limitations on the scope or nature of the test.

**Risk Frameworks**

Similar to (and, in some cases, overlapping with) the security control frameworks mentioned earlier in this domain, the security practitioner may also make use of risk frameworks to optimize the
organization’s response to risk. In many mature organizations, this effort defines the organization’s strategy in terms of business risks and opportunities and is often referred to as enterprise risk management (ERM).

Many different standards bodies and industry-specific entities publish ERM guidance and documentation. These include (but are not limited to):

- **ISO**: Standards 31000 (Risk Management—Principles and Guidelines) and 27005 (Information technology—Security techniques—Information security risk management) both discuss risk from a holistic organizational perspective (the former) and as specifically related to IT security (the latter). Standard 27001 is also endorsed by ENISA (the European Union Agency for Network and Information Security) as a means of managing risk.

- **COSO**: The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was formed in the wake of dramatic and severe financial industry scandals in the United States in the 1980s, as a body to suggest guidelines and practices to address financial reporting irregularities and fraud. Since that time, its publications have been widely accepted and adopted by many large companies. In 2004, COSO published the first version of its Enterprise Risk Management - Integrated Framework; this document was updated in 2017 and is seen as a definitive guide to the topic.

- **ISACA**: Publishes the RISK IT framework, which is described by ISACA as connecting risk management from a strategic perspective with risk-related IT management.

- **NIST**: Special Publication (SP) 800-37, mentioned earlier in this domain, is the Risk Management Framework (RMF), which is extremely influential and important for how U.S. federal government agencies address risk.

The candidate is advised to research the topic of risk frameworks; however, of the ones listed here, only the NIST RMF is available without payment.

**Apply Risk-Based Management Concepts to the Supply Chain**

An organization rarely operates wholly alone; there are many dependencies and interconnections organizations have with their entire supply chain: the organization’s suppliers, vendors, contractors, and customers.

It is imperative that the organization applies the same risk-management methodologies and perspective to this supply chain as the organization
did for its own internal operations. This may include the organization performing the following for each entity within the supply chain:

- Governance review
- Site security survey
- Formal security audit
- Penetration testing

However, in many cases, this is untenable, and sometimes it can create additional liability issues for both parties. Instead, organizations often rely on audit reports prepared by certified third parties to properly evaluate the entities within the organization’s supply chain. This has notably been the case with managed cloud services, where the cloud customer often does not even know the physical location of the cloud data center and must rely on external validation of the provider’s security.

There are a variety of standards and audit methodologies for assessing the security of external organizations. These include, but are not limited to the following:

- **ISO-certified audits**: Each ISO standard can be assessed by an accredited auditor, and the target organization can earn certification by successfully passing this audit.

- **CSA STAR evaluation**: As mentioned previously in this domain, the CSA offers a registration program for cloud providers called STAR. STAR can be self-administered by the target organization or conducted by a certified external auditor, depending on the STAR Level the target organization seeks.

- **AICPA SSAE 16 SOC reports**: The American Institute of Certified Public Accountants (AICPA) created the Statement on Standards of Attestation Engagements (SSAE) 16 standard as a response to prevailing federal legislation in the United States (specifically, the Sarbanes–Oxley Act, referred to as SOX). The SSAE 16 standard details three types of reports intended for different uses; these are the SOC reports. While the SSAE 16 standard is designed for publicly traded corporations, it has come into wide use by organizations of all types.

**Understand and Apply Threat Modeling Concepts and Methodologies**

As explained in this domain, a threat is something that might cause a threat to be realized. To anticipate and counter anthropomorphic threats, the security industry uses a technique called threat modeling,
which entails looking at an environment, system, or application from an attacker’s viewpoint and trying to determine vulnerabilities the attacker would exploit. The end state of this process is addressing each of the vulnerabilities discovered during threat modeling to ensure an actual attacker cannot use them.

In many threat modeling techniques, an abstract, nontechnical abstraction of the target (whether it is an organization or an IT system/application) is necessary before reviewing the details of the target itself. Workflow diagrams (also referred to as dataflow diagrams or flowcharts) are frequently used for the purpose; the threat modeling team creates a conceptual view of how the target actually functions—how data and processes operate in the target from start to finish. This allows the threat modeling team to understand where an attacker might affect the target, by understanding potential locations (in time, space, and the process) of vulnerabilities.

In some threat models used for specific targets (systems/applications, instead of the overall organization), another element is used (mostly in addition to, not in lieu of, the abstract); incorporating those same threat modeling techniques into the detailed specifics of the target. With this technique, designers can identify and troubleshoot potential vulnerabilities during the development and acquisition of the target instead of waiting until the target reaches the production environment. This practice (securing a system/application) during development is less expensive and time-consuming than addressing issues after the item has entered production.

The candidate should certainly be familiar with one particular threat modeling tool: STRIDE. STRIDE, created by Microsoft, is actually a threat classification system used to inform software developers during the development process. These are the elements of STRIDE:

- **Spoofing identity**: the type of threat wherein an attacker poses an entity other than the attacker, often as an authorized user.
- **Tampering with data**: when the attacker attempts to modify the target data in an unauthorized way.
- **Repudiation**: when the attacker, as a participant of a transaction, can deny (or conceal) the attacker’s participation in that transaction.
- **Information disclosure**: just like it sounds, this category can include both inadvertent release of data (where an authorized user discloses protected data accidentally to unauthorized users, or gains access to material that their authorization should not allow) and malicious access to data (an attacker getting unauthorized access).
• **Denial of service (DoS):** an attack on the availability aspect of the CIA triad; creating a situation in the target where authorized users cannot get access to the system/application/data.

• **Elevation of privilege:** when an attacker not only gains access to the target but can attain a level of control with which to completely disable/destroy the entire target system.

NOTE: The candidate should know each of the elements of the STRIDE model; as the term is an acronym, it is not exceptionally difficult. However, some of the concepts seem to have been worded in such a way as to force them into an acronym, which makes them slightly differently worded in a way that varies from other industry usage (for instance, the term “nonrepudiation” is commonly used; the STRIDE variant, “repudiation” is specific to STRIDE).

Other threat models include:

• **OCTAVE:** Created by Carnegie-Mellon University, the OCTAVE model is designed for viewing the overall risk of IT systems across an organization. Published with two variants, OCTAVE for large organizations, OCTAVE-S for smaller operations. [http://www.cert.org/resilience/products-services/octave/](http://www.cert.org/resilience/products-services/octave/)

• **Trike:** An open-source methodology and toolset from the Massachusetts Institute of Technology (MIT). Has not been updated/revised for some time. [http://octotrike.org/home.shtml](http://octotrike.org/home.shtml)

**Risks Associated with Hardware, Software, and Services**

The following is a non-comprehensive list of common risks:

**Hardware**

• **Theft:** A box that can be touched can be owned; almost no technical controls can withstand physical access to a device, so physical security of all components is crucial, as is ensuring that your personnel are screened and monitored.

• **Natural disasters:** Physical devices are subject to physical impact, and natural disasters pose a continual risk to operations. Of particular concern is flooding as water is so hostile to IT components, but a great many disasters can affect hardware, such as hurricanes, tornadoes, earthquakes, blizzards, and so on.
Fire: While fire can result from natural disasters, it can also be a localized threat to the internal environment of a data center. The impact of combatting fire can be just as detrimental to physical IT components as the fire itself. This topic is addressed in more detail in Domain 7.

Software

- **Defects:** Bugs and improperly designed functions that can be exploited by attackers. Defects that are discovered by attackers after a product has shipped and been put into production, without the knowledge of either the vendor or users, are known as “zero-day” exploits, as attackers can use these vulnerabilities indiscriminately for the time it takes until a patch or solution is created to resolve the defect.

- **Lack of security:** Software that is not designed with proper security controls is prolific and poses a significant risk to the organization. Including security as an aspect of software development and acquisition is crucial and discussed in depth in Domain 8.

- **Malicious software (malware):** Software can be used as an attack vector by people with malicious intent for a variety of potential outcomes that affect every aspect of the CIA triad. Malware includes worms, viruses, and Trojan horse programs.

Services

- **Denial of service (DoS) and distributed denial of service (DDoS):** A DoS attack is launched by a malicious person trying to affect the availability of systems or data. While this can take almost any form (including physical), it often manifests as an attack on (or using) native IT services, such as communication protocols. A DDoS attack amplifies the attack source through the attacker’s use of many disparate machines to focus on the target. Modern DDoS attacks have used exponentially more attack devices than were expected to a significant deleterious effect.

- **“Man in the middle”:** Attacks on active communications are referred to as “man in the middle,” where the attacker positions themself (physically or logically) between parties engaged in a communications session. This can be used to affect every aspect of the CIA triad.

- **Social engineering:** If authorized use can be considered a form of service, then undermining authorized users themselves can be considered a service attack; this is called “social engineering.”
Subverting the user can be done in many ways and often exploits common human behaviors and emotions. Techniques include blackmail, bluster, browbeating, bribery, and an appeal to aid.

This list is in no way comprehensive and is only offered as a cursory overview.

Minimum Security Requirements
To provide appropriate levels of security, a fundamental understanding of the desired outcomes is necessary. Security professionals achieve this by gathering a set of minimum security requirements to use as a goal. This minimum set of requirements should be created for every level granularity in an operation: the organization as a whole (where the minimum security requirements become the level of acceptable risk), the overall IT environment, each network that is included in the environment, each system in each network, and even each component. Moreover, this practice (gathering minimum security requirements) should not be limited only to IT and data activity, but it should also be included in project management and process functions.

Some hints for effectively gathering minimum security requirements:

- Involve stakeholders in the development/acquisition/planning process as soon as possible (close to the start of the endeavor).
- Ensure that requirements are specific, realistic, and measurable.
- Record and document all elements of the discussion and outcome.
- When soliciting input from the customer, restate your understanding of their requests back to them to confirm what they intended to say and what you comprehend.
- Don’t choose tools or solutions until the requirements are understood; too often in our field, we already have a preferred technology in mind when starting a project, when we should instead only select a specific product once we fully comprehend the objectives. Otherwise, we tend to allow the technology to drive business functions, instead of the other way around.
- If possible, create diagrams, models, and prototypes to solidify mutual understanding of the requirements before commencing full-scale development and production.
Service Level Requirements

When an organization uses an external provider for managed services (for example, a cloud service, or a contractor that maintains the organization’s data center), the parties must establish a mutual understanding of exactly what will be provided, under which terms, and at what times. This should include a detailed description of both performance and security functions. As with other projects, the organization has to establish a set of minimum requirements for this effort to be successful; in this type of case, however, the organization is not usually able to dictate requirements unilaterally and must instead cooperate with the provider.

Together, the parties will construct a business contract explicitly stating the terms of the arrangement. One part of this contract should be the service-level agreement (SLA), which defines the minimum requirements and codifies their provision. Every element of the SLA should include a discrete, objective, numeric metric with which to judge success or failure, otherwise, the SLA implementation will not be fair or reasonable for either party.

For example, an SLA element that states, “There will be excellent uptime for the duration of the service,” is not adequate; attorneys could spend months debating the meaning of “excellent” in the event the parties don’t agree on sufficiency of service during a given period. Instead, an element stating, “The customer will have continual access to the service during the period of delivery; interruption lasting more than five (5) seconds per period will result in failure,” would be preferable.

The strength of the SLA is its use as a payment discriminator; usually, SLAs are created with contractual stipulations such that a failed SLA element will result in a credit applied to the customer’s account. This incentivizes the provider to meet the terms of the SLA and mollifies the customer if any particular aspect of the service does not fully meet the customer’s needs.

NOTE: SLAs best serve recurring, continual requirements not singular or infrequent events. For instance, a weekly performance report might be included in the SLA, but a disaster response/recovery metric probably is not suited for the SLA. However, specific terms for addressing uncommon events like disaster response/recovery can and should be included in the contract, even if they are not in the SLA.

Activity: SLA or Not?

You are the security manager for a chain of retail stores. Your company recently entered into negotiation with an external provider of data archiving services, which will securely store your nonproduction data for long-term purposes. You are asked by senior management to review the contract terms and SLA.
Instructions
As group, using the criteria described in this module, determine whether each of the following elements should be included in an SLA, stated elsewhere in the managed service contract, or not included at all. You have 10 minutes

a. The amount of data the customer can move to the archive daily
b. The format in which the data will stored
c. The media which will be used to store the data
d. Security methods used to routinely protect the data in storage
e. Volume of storage made available to the customer
f. Results of routine data integrity checks

Answers:

a. **SLA**—a discrete, objective, numeric metric can be applied, and this is a regularly-occurring activity
b. **Contract**—this is not a recurring activity and can be stated just once elsewhere in the contract
c. **Contract**—this is not a recurring activity and can be stated just once elsewhere in the contract
d. **Neither**—disclosing this information makes the service less secure and should not be shared outside the provider’s organization
e. **Contract**—this is not a recurring activity and can be stated just once elsewhere in the contract
f. **SLA**—a discrete, objective, numeric metric can be applied, and this is a regularly-occurring activity
Module 4: Compliance Requirements

Module Objectives

1. Recognize the various forms of compliance requirements (laws/regulations, standards, and contracts).
2. Understand the concept of regulatory compliance, especially in the context of modern privacy requirements, and identify typical regulations encountered in practice.
3. Identify common privacy terms used in current personal data protection laws worldwide.
Contractual, Legal, Industry Standards, and Regulatory Requirements

Every organization operates under some type of external mandate. This mandate can come in the form of simple contracts, as part of the organization’s interactions with suppliers and customers; the organization is compelled to fulfill their contractual obligations. Mandates can also come in the form of governmental imposition; governments create regulations, either through legislative or administrative means, and organizations must adhere to the regulations relevant to the industry and manner in which the organization operates. There are also traditional and cultural mandates, arising in every society; some of these take the form of standards, which each organization is held to by custom and, in some jurisdictions, by legal precedent and liability.

Compliance is adherence to a mandate, regardless of the source. Almost every modern organization is required to demonstrate compliance to the various mandates the organization is subject to. Compliance is used in our industry as a term that means both the action on the part of the organization to fulfill the mandate and the tools, processes, and documentation that demonstrate adherence.

Many modern mandates address a specific need: personal privacy. Privacy is the right of a human being to control the manner and extent to which information about him or her is distributed. Privacy mandates take all forms: contractual, regulatory, and customary.

Organizations are often reviewed to determine compliance with applicable mandates. Often, the tools, processes, and activities used to perform compliance reviews are referred to as audits (or auditing).

Contractual Mandates

A contract is an agreement between parties requiring them to perform in some way and the terms for performance. Contracts are an instrumental tool in business where the contract obligates the organization; contracts are either used or implicit in every business transaction. Contracts could be as simple as the exchange of money for a product, or a complicated, long-term arrangement requiring hundreds of pages of contract documentation.

An organization enters into a contract voluntarily, and law and custom dictate that every party to a contract will fulfill the requirements of the
contract unless they are unable to do so. The importance of contracts has been codified in most countries as law, to the extent that any party not fulfilling their contractual obligations may be forced to do so (or pay recompense) if the other party/parties to the contract seek relief from the courts.

In many cases, parties to a contract may have the right to review the progress and activity of each other to ensure the terms of the contract are being met (this is also stipulated in the contract). This may involve inspection of raw data, a measure of some performance, or audits; these actions may be performed by the parties to the contract or by external third parties on their behalf.

The candidate should be familiar with one widely used contract as it is the basis for a great deal of work performed in the IT security industry: the contract between entities that issue credit cards in the United States and any entity that accepts those cards as a form of payment (referred to as “merchants”). This contract is promulgated by the Payment Card Industry (PCI) Security Standards Council; the Council publishes and enforces the Payment Card Industry Data Security Standard (PCI DSS).

The Data Security Standard (DSS) is generally view by those in the industry as comprehensive and fairly well designed and administered. It is also a mandate with significant consequences: any merchant that doesn’t properly comply with the DSS can be assessed a fee by the Council, and the Council reserves the right to revoke any merchant’s ability to accept credit card payment for continued or exacerbated noncompliance. For many merchants, losing the ability to receive credit card payments would be fatal to their operations, so they are extremely motivated to remain compliant.

Under PCI DSS, merchants are categorized into four Merchant Levels, according to the number of credit card transactions the merchant is party to annually. Merchants are required to subscribe to the security control areas and processes described in the DSS. For the most part, the DSS involves protecting privacy data related to the cardholder (the cardholder’s name, card number, billing address, etc.), including mandating some mechanisms for ensuring protection, such as encryption or tokenization.

Other elements of the DSS exist to protect the financial institution that has issued the card, especially in transactional activity. For instance, merchants are not allowed to store the Card Verification Value (CVV) number that appears on the card itself, for any length of time; the CVV can only be used during the transaction.
Legal Standards
Legal standards are set by courts in decisions that set precedent; that is, the judgments a court has made previously become the standard of acceptable practice for future behavior. This precedent informs other courts in making determinations, for instance, of reasonable expectations for parties to a contract—the due care mentioned earlier in this domain.

Organizations use these standards in the formulation of their own strategy and governance as a means of setting acceptable risk. When a court makes a decision about due care, organizations that will be subject to similar circumstances make plans according to that standard out of recognition of liability they might face for noncompliance.

For example, an organization perceives and understands judgments for and against other organizations in the same industry or line of work and acts accordingly. If an organization is involved in manufacturing and is performing a cost-benefit analysis regarding how to dispose of industrial waste, senior management might consider using a non-certified disposal method to cut costs. However, management would be wise to consider, in addition to other externalities and mandates, how other manufacturing operations have been treated by the courts when those manufacturers engaged in similar activity.

NOTE: On this particular example, there are, of course, other external mandates as mentioned, notably legislative and statutory mandates related to manufacturing waste disposal that require the attention of senior management, as well as the pertinent legal standards.

Industry Standards
As can be understood from the term, industry standards are set for and by the organizations involved and associated with a given field of endeavor. For instance, in the field of IT security, (ISC)² is a standard body that creates, maintains, and determines eligibility for certifications of professional practitioners. Absent other mandates, this standard has no inherent legal force but has weight and credence lent it by recognition from industry participants.

Through time and use, industry standards may take on legal substance when recognized by the court as credible and recognized. For instance, when an organization is defending itself in court against accusations of negligence in the due care for delivery of IT security, the organization can present the experience and professional
certifications of the organization’s IT security personnel as demonstration of the organization’s due diligence: the organization hired certified personnel, thus displaying due diligence in provision of security services.

Regulators (described in detail in a later section of this module) may also recognize industry standards are sufficient for meeting regulatory compliance requirements, especially in the absence of clear statutory or administrative law guidance for a particular topic.

Some industry standards (including mention of those that were introduced earlier in this domain) that the candidate may find useful:

- **ISO**: The International Standards Organization, which publishes industry standards for almost every type of endeavor and operation, is recognized globally for the comprehensiveness and credibility of its standards. They are, however, expensive.

- **CSA STAR**: The Cloud Security Alliance (CSA) program for certifying managed cloud service providers.

- **Uptime Institute**: Certification program for data centers, usually involving managed services, describing the center’s capability to support the availability aspect of the CIA triad.

- **SSAE 16**: Audit standard, designed for publicly-traded corporations but widely used by many organizations, including managed cloud providers, devised by the American Institute of Certified Public Accountants (AICPA).

### Regulatory Standards

Regulations are mandates set by government bodies. Regulations can be created by legislative or administrative action. Regulated organizations are subject to oversight by representatives from the applicable regulatory agencies (called “regulators”). Punishment for failure to comply can result in fines, court orders for performance, and in some cases imprisonment for principals of the organization.

A list of some regulations the candidate should be familiar with:

- **General Data Protection Regulation (GDPR)**: From the European Union, addresses personal privacy, deeming it an individual human right. Currently perhaps the single most powerful and influential regulations associated with IT and data security in the world, influencing laws in many other countries and regions. GDPR and some associated programs is discussed in more depth in Module 5 of this domain.

- **Health Insurance Portability and Accountability Act (HIPAA)**: An American federal law that affects medical providers,
and includes stipulations regarding the collection and dissemination of health-related personal information, referred to in the Act and the industry as “electronic protected health information (ePHI).”

- **Graham–Leach–Bliley Act (GLBA):** A federal U.S. law that allowed banks to merge with insurance providers and includes protection, collection, and dissemination requirements for the personal information of individual account holders.

- **Sarbanes–Oxley Act (SOX):** Created by the U.S. Congress as a response to a series of dramatic frauds committed by publicly traded corporations in the 1990s. Contains security, privacy, and availability requirements of great interest to IT security practitioners as resulting industry standards (specifically, SSAE 16) created as a mechanism for SOX audits have been accepted by many organizations, beyond publicly traded corporations.

- **Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA):** Is severely restrictive of privacy data collection and dissemination and requires intense security for such data.

- **Federal Information Systems Management Act (FISMA):** A U.S. national law applicable only to federal government agencies, requires all covered entities to comply with NIST guidance and standards for securing IT environments under those agencies’ control. FedRAMP, the Federal Risk and Authorization Management Program, is a wide-reaching mandate that is a corollary to this law and stipulates security requirements for managed service providers that want to sell to federal government customers.

- **Personal Data Protection Law (Argentina):** Argentina’s statute that creates a legal environment in that country that directly adheres and supports the GDPR.

- **Personal Data Protection Law (Singapore):** Singapore’s national law addressing all privacy data collected, processed, and disseminated in or through that country.

- **The Privacy Act:** Sometimes confused with the American law of the same name, this is Australia’s law that dictates how personal information in Australia may be collected and disseminated.

- **Act on Protection of Personal Information (APPI):** A Japanese national law that covers business organizations that hold personal data on 5,000 or more individuals.
Common Privacy Law Tenets

Many privacy laws address similar concepts associated with individual personal data, that have become common globally. The candidate should be familiar with these general concepts:

- **Notification**: The data subject (the individual human related to the personal data in question) should be notified before any of their personal data is collected or created.

- **Participation**: The subject should have the option not to take part in the transaction, if the subject chooses not to share their personal data.

- **Scope**: Any personal data collected or created should be for a specific purpose; this purpose should be legal and ethical and be included in the notification aspect of the transaction, as well as inform the limitation aspect.

- **Limitation**: Any personal data should only be used for the purpose identified in the scope aspect of the transaction; any additional use would require repeating the notification and participation aspects.

- **Accuracy**: Any personal data should be factual and current; data subjects should have a means to correct/edit any information about the subject in a simple, timely manner.

- **Retention**: Personal data should not be kept any longer than is necessary for the purpose, or as required by applicable law.

- **Security**: Any entity that has possession of personal data is responsible for protecting it.

- **Dissemination**: Any entity that has possession of personal data should not share it with any other entity, nor release it, without the express permission of the data subject and in accordance with applicable law.