CompTIA

The Official CompTIA

Security+ Study Guide

Exam SY0-701

Official CompTIA Content Series for CompTIA Performance Certifications

The Official CompTIA Security+ Study Guide (Exam SY0-701)

Course Edition: 2.0

Acknowledgments

James Pengelly, Author
Gareth Marchant, Author

Michael Olsen, Director, Content Development
Danielle Andries, Senior Manager, Content Development

Notices

Disclaimer

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

Trademark Notice

Copyright Notice

Table of Contents

About This Course

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations; its industry-leading IT certifications are an important part of that mission. CompTIA's Security+ certification is a global certification that validates the foundational cybersecurity skills necessary to perform core security functions and pursue an IT security career.

> This exam will certify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents.
>
> Security+ is compliant with ISO 17024 standards. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.
>
> *CompTIA Security+ Exam Objectives*

Course Description

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-701) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of IT security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your cybersecurity skill set so that you can confidently perform your duties in any entry-level security role.

On course completion, you will be able to do the following:

- Summarize fundamental security concepts.
- Compare threat types.
- Explain appropriate cryptographic solutions.
- Implement identity and access management.
- Secure enterprise network architecture.
- Secure cloud network architecture.
- Explain resiliency and site security concepts.
- Explain vulnerability management.
- Evaluate network security capabilities.
- Assess endpoint security capabilities.
- Enhance application security capabilities.
- Explain incident response and monitoring concepts.
- Analyze indicators of malicious activity.

- Summarize security governance concepts.
- Explain risk management processes.
- Summarize data protection and compliance concepts.

Target Student

The Official CompTIA Security+ (Exam SY0-701) is the primary course you will need to take if your job responsibilities include safeguarding networks, detecting threats, and securing data in your organization. You can take this course to prepare for the CompTIA Security+ (Exam SY0-701) certification examination.

Prerequisites

To ensure your success in this course, you should have a minimum of two years of experience in IT administration with a focus on security, hands-on experience with technical information security, and a broad knowledge of security concepts. CompTIA A+ and CompTIA Network+, or the equivalent knowledge, is strongly recommended.

The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: www.comptia.org/training/resources/exam-objectives.

How to Use the Study Notes

The following notes will help you understand how the course structure and components are designed to support mastery of the competencies and tasks associated with the target job roles and will help you to prepare to take the certification exam.

As You Learn

At the top level, this course is divided into **lessons**, each representing an area of competency within the target job roles. Each lesson is composed of a number of topics. A **topic** contains subjects that are related to a discrete job task, mapped to objectives and content examples in the CompTIA exam objectives document. Rather than follow the exam domains and objectives sequence, lessons and topics are arranged in order of increasing proficiency. Each topic is intended to be studied within a short period (typically 30 minutes at most). Each topic is concluded by one or more activities, designed to help you to apply your understanding of the study notes to practical scenarios and tasks.

In addition to the study content in the lessons, there is a glossary of the terms and concepts used throughout the course. There is also an index to assist in locating particular terminology, concepts, technologies, and tasks within the lesson and topic content.

In many electronic versions of the book, you can click links on key words in the topic content to move to the associated glossary definition, and on page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your eBook viewing software.

Watch throughout the material for the following visual cues.

A **Note** provides additional information, guidance, or hints about a topic or task.

A **Caution** note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

Following the lesson content, you will find a table mapping the lessons and topics to the exam domains, objectives, and content examples. You can use this as a checklist as you prepare to take the exam and to review any content that you are uncertain about.

As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Lesson 1

Summarize Fundamental Security Concepts

LESSON INTRODUCTION

Security is an ongoing process that includes assessing requirements, setting up organizational security systems, hardening and monitoring those systems, responding to attacks in progress, and deterring attackers. If you can summarize the fundamental concepts that underpin security functions, you can contribute more effectively to a security team. You must also be able to explain the importance of compliance factors and best practice frameworks in driving the selection of security controls and how departments, units, and professional roles within different types of organizations implement the security function.

Lesson Objectives

In this lesson, you will do the following:

- Summarize information security concepts.
- Compare and contrast security control types.
- Describe security roles and responsibilities.

Topic 1A

Security Concepts

EXAM OBJECTIVES COVERED
1.2 Summarize fundamental security concepts.

To be successful and credible as a security professional, you should understand security in business starting from the ground up. You should know the key security terms and ideas used by security experts in technical documents and trade publications. Security implementations are constructed from fundamental building blocks, just like a large building is built from individual bricks. This topic will help you understand those building blocks so that you can use them as the foundation for your security career.

Information Security

Information security (infosec) refers to the protection of data resources from unauthorized access, attack, theft, or damage. Data may be vulnerable because of the way it is stored, transferred, or processed. The systems used to store, transmit, and process data must demonstrate the properties of security. Secure information has three properties, often referred to as the **CIA Triad**:

- **Confidentiality** means that information can only be read by people who have been explicitly authorized to access it.
- **Integrity** means that the data is stored and transferred as intended and that any modification is authorized.
- **Availability** means that information is readily accessible to those authorized to view or modify it.

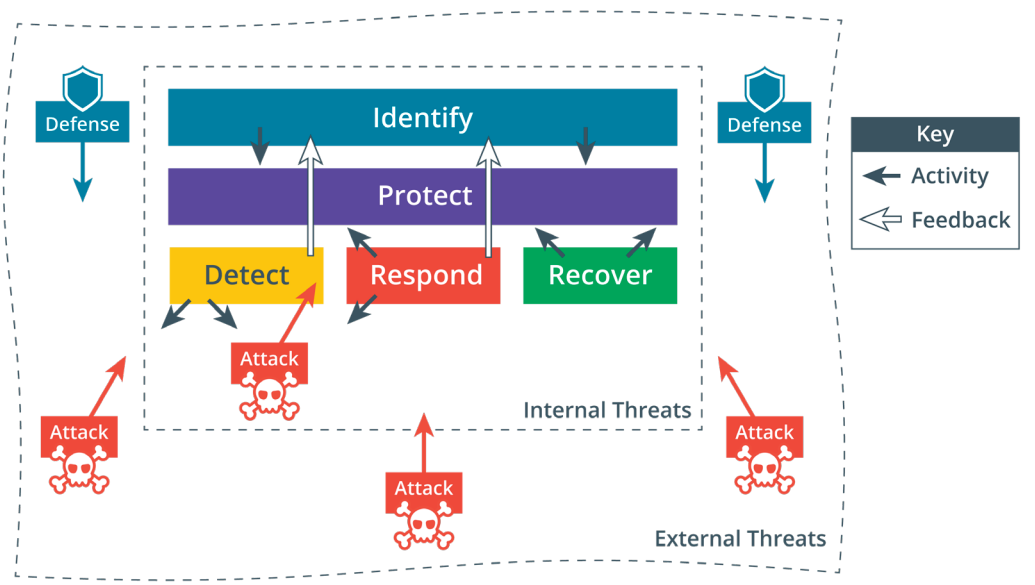
The triad can also be referred to as "AIC" to avoid confusion with the Central Intelligence Agency.

Some security models and researchers identify other properties of secure systems. The most important of these is non-repudiation. **Non-repudiation** means that a person cannot deny doing something, such as creating, modifying, or sending a resource. For example, a legal document, such as a will, must usually be witnessed when it is signed. If there is a dispute about whether the document was correctly executed, the witness can provide evidence that it was.

Cybersecurity Framework

Within the goal of ensuring information security, cybersecurity refers specifically to provisioning secure processing hardware and software. Information security and cybersecurity tasks can be classified as five functions, following the framework developed by the **National Institute of Standards and Technology (NIST)** (nist.gov/cyberframework/online-learning/five-functions):

- **Identify**—develop security policies and capabilities. Evaluate risks, threats, and vulnerabilities and recommend security controls to mitigate them.
- **Protect**—procure/develop, install, operate, and decommission IT hardware and software assets with security as an embedded requirement of every stage of this operation's lifecycle.
- **Detect**—perform ongoing, proactive monitoring to ensure that controls are effective and capable of protecting against new types of threats.
- **Respond**—identify, analyze, contain, and eradicate threats to systems and data security.
- **Recover**—implement cybersecurity resilience to restore systems and data if other controls are unable to prevent attacks.



Core cybersecurity tasks.

NIST's framework is just one example. There are many other ***cybersecurity frameworks (CSF)****.*

Gap Analysis

Each security function is associated with a number of goals or outcomes. For example, one outcome of the Identify function is an inventory of the assets owned and operated by the company. Outcomes are achieved by implementing one or more **security controls**.

Numerous categories and types of security controls cover a huge range of functions. This makes selection of appropriate and effective controls difficult.

A cybersecurity framework guides the selection and configuration of controls. Frameworks are important because they save an organization from building its security program in a vacuum, or from building the program on a foundation that fails to account for important security concepts.

The use of a framework allows an organization to make an objective statement of its current cybersecurity capabilities, identify a target level of capability, and prioritize investments to achieve that target. This gives a structure to internal risk management procedures and provides an externally verifiable statement of regulatory compliance.

Gap analysis is a process that identifies how an organization's security systems deviate from those required or recommended by a framework. This will be performed when first adopting a framework or when meeting a new industry or legal compliance requirement. The analysis might be repeated every few years to meet compliance requirements or to validate any changes that have been made to the framework.

For each section of the framework, a gap analysis report will provide an overall score, a detailed list of missing or poorly configured controls associated with that section, and recommendations for remediation.

Function	Controls (Actual/Required)	CIA Triad Risk Levels	Target Remediation
Identify (10/16)	Asset Management (4/6)	C : 6 I : 6 A : 6	Q4
	Governance (3/4)	C : 6 I : 6 A : 1	Q3
	Risk Assessment (3/6)	C : 6 I : 6 A : 3	Q3
Protect (8/16)	Identity and Access Management (5/8)	C : 9 I : 9 A : 4	Q1
	Data Security (3/8)	C : 9 I : 9 A : 4	Q1

Advanced capability
Intermediate capability
No/basic capability

Summary of gap analysis findings showing number of recommended controls not implemented per function and category; plus risks to confidentiality, integrity, and availability from missing controls; and target remediation date.

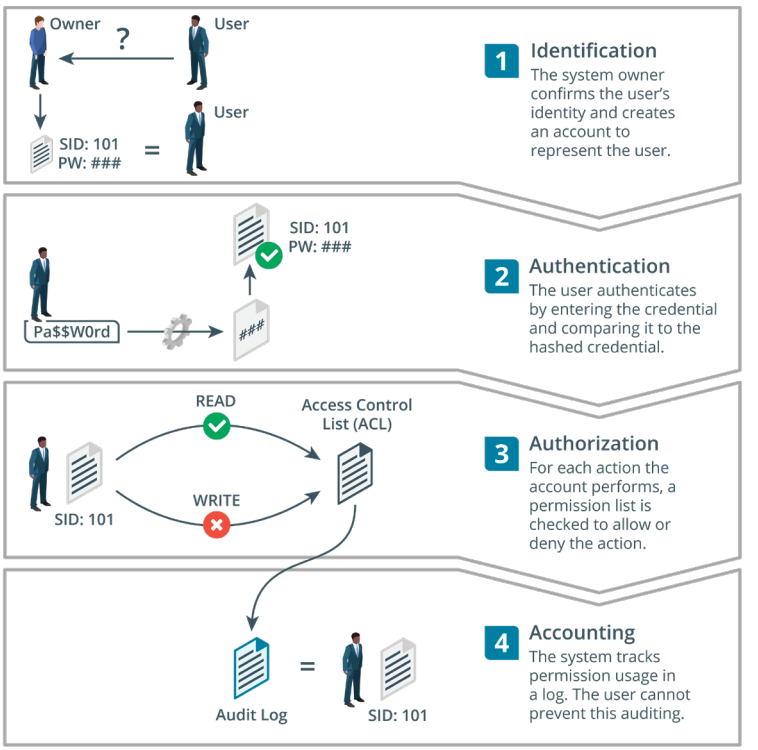
While some or all work involved in gap analysis could be performed by the internal security team, a gap analysis is likely to involve third-party consultants. Frameworks and compliance requirements from regulations and legislation can be complex enough to require a specialist. Advice and feedback from an external party can alert the internal security team to oversights and to new trends and changes in best practice.

Access Control

An access control system ensures that an information system meets the goals of the CIA triad. Access control governs how subjects/principals may interact with objects. Subjects are people, devices, software processes, or any other system that can request and be granted access to a resource. Objects are the resources. An object could be a network, server, database, app, or file. Subjects are assigned rights or permissions on resources.

Modern access control is typically implemented as an **identity and access management (IAM)** system. IAM comprises four main processes:

- **Identification**—creating an account or ID that uniquely represents the user, device, or process on the network.
- **Authentication**—proving that a subject is who or what it claims to be when it attempts to access the resource. An authentication factor determines what sort of credential the subject can use. For example, people might be authenticated by providing a password; a computer system could be authenticated using a token such as a digital certificate.
- **Authorization**—determining what rights subjects should have on each resource, and enforcing those rights. An authorization model determines how these rights are granted. For example, in a discretionary model, the object owner can allocate rights. In a mandatory model, rights are predetermined by system-enforced rules and cannot be changed by any user within the system.
- **Accounting**—tracking authorized usage of a resource or use of rights by a subject and alerting when unauthorized use is detected or attempted.



Differences among identification, authentication, authorization, and accounting. (Images © 123RF.com.)

*The servers and protocols that implement these functions can also be referred to as **authentication, authorization, and accounting (AAA)**. The use of IAM to describe enterprise security workflows is becoming more prevalent as the importance of the identification process is better acknowledged.*

For example, if you are setting up an e-commerce site and want to enroll users, you need to select the appropriate controls to perform each function:

- **Identification**—ensure that customers are legitimate. For example, you might need to ensure that billing and delivery addresses match and that they are not trying to use fraudulent payment methods.
- **Authentication**—ensure that customers have unique accounts and that only they can manage their orders and billing information.
- **Authorization**—rules to ensure customers can place orders only when they have valid payment mechanisms in place. You might operate loyalty schemes or promotions that authorize certain customers to view unique offers or content.
- **Accounting**—the system must record the actions a customer takes (to ensure that they cannot deny placing an order, for instance).

Remember that these processes apply both to people and to systems. For example, you need to ensure that your e-commerce server can authenticate its identity when customers connect to it using a web browser.

Review Activity:

Security Concepts

Answer the following questions:

1. **What are the properties of a secure information processing system?**

2. **What term is used to describe the property of a secure network where a sender cannot deny having sent a message?**

3. **A company provides a statement of deviations from framework best practices to a regulator. What process has the company performed?**

4. **What process within an access control framework logs actions performed by subjects?**

5. **What is the difference between authorization and authentication?**

6. **How does accounting provide non-repudiation?**

Topic 1B

Security Controls

EXAM OBJECTIVES COVERED

1.1 Compare and contrast various types of security controls.

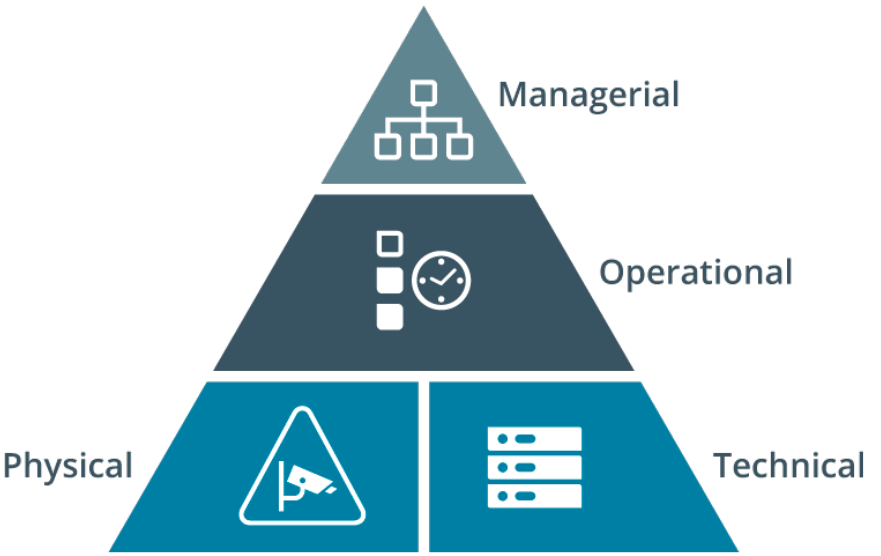
Information security and cybersecurity assurance is met by implementing security controls. By identifying basic security control types, you will be better prepared to select and implement the most appropriate controls for a given scenario. You should also be able to describe how specific job roles and organizational structures can implement a comprehensive security program for organizations.

Security Control Categories

Information and cybersecurity assurance usually takes place within an overall process of business risk management. Implementation of cybersecurity functions is often the responsibility of the IT department. There are many different ways of thinking about how IT services should be governed to fulfill overall business needs. Some organizations have developed IT service frameworks to provide best practice guides to implementing IT and cybersecurity. These frameworks can shape company policies and provide checklists of procedures, activities, and technologies that represent best practice. Collectively, these procedures, activities, and tools can be referred to as security controls.

A **security control** is designed to give a system or data asset the properties of confidentiality, integrity, availability, and non-repudiation. Controls can be divided into four broad categories based on the way the control is implemented:

- **Managerial**—the control gives oversight of the information system. Examples could include risk identification or a tool allowing the evaluation and selection of other security controls.
- **Operational**—the control is implemented primarily by people. For example, security guards and training programs are operational controls.
- **Technical**—the control is implemented as a system (hardware, software, or firmware). For example, firewalls, antivirus software, and OS access control models are technical controls.
- **Physical**—controls such as alarms, gateways, locks, lighting, and security cameras that deter and detect access to premises and hardware are often placed in a separate category to technical controls.



Categories of security controls

Although it uses a different scheme, be aware of the way the National Institute of Standards and Technology (NIST) classifies security controls (csrc.nist.gov/publications/detail/sp/800-53/rev-5/final).

Security Control Functional Types

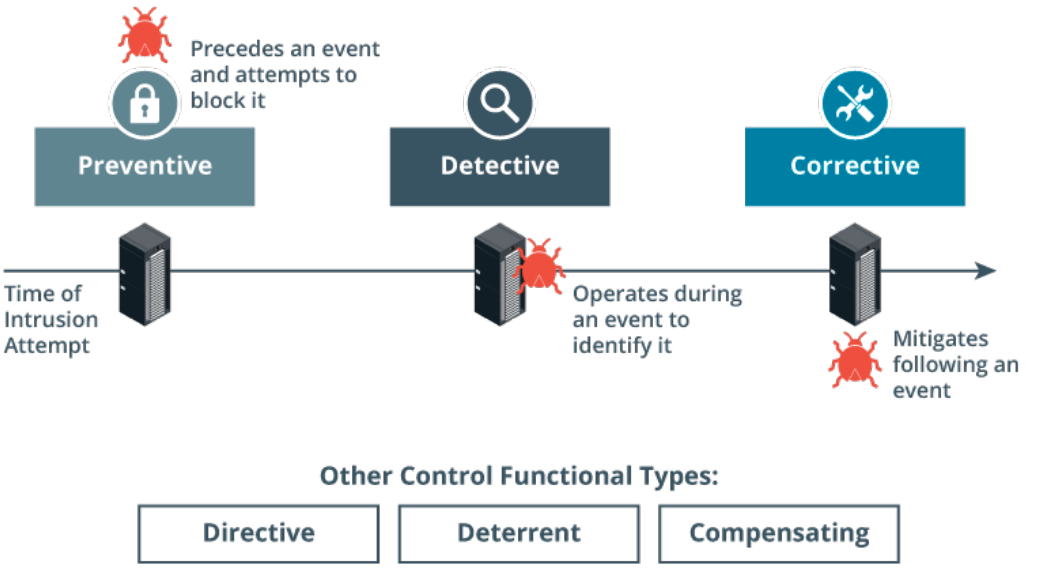
As well as a category, a security control can be defined according to the goal or function it performs:

- **Preventive**—the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventive control operates before an attack can take place. **Access control lists (ACL)** configured on firewalls and file system objects are preventive-type technical controls. Antimalware software acts as a preventive control by blocking malicious processes from executing.
- **Detective**—the control may not prevent or deter access, but it will identify and record an attempted or successful intrusion. A detective control operates during an attack. Logs provide one of the best examples of detective-type controls.
- **Corrective**—the control eliminates or reduces the impact of a security policy violation. A corrective control is used after an attack. A good example is a backup system that restores data that was damaged during an intrusion. Another example is a patch management system that eliminates the vulnerability exploited during the attack.

While most controls can be classed functionally as preventive, detective, or corrective, a few other types can be used to define other cases:

- **Directive**—the control enforces a rule of behavior, such as a policy, best practice standard, or standard operating procedure (SOP). For example, an employee's contract will set out disciplinary procedures or causes for dismissal if they do not comply with policies and procedures. Training and awareness programs can also be considered as directive controls.

- **Deterrent**—the control may not physically or logically prevent access, but it psychologically discourages an attacker from attempting an intrusion. This could include signs and warnings of legal penalties against trespass or intrusion.
- **Compensating**—the control is a substitute for a principal control, as recommended by a security standard, and affords the same (or better) level of protection but uses a different methodology or technology.



Functional types of security controls. (Images © 123RF.com.)

Information Security Roles and Responsibilities

A security policy is a formalized statement that defines how security will be implemented within an organization. It describes the means the organization will take to protect the confidentiality, availability, and integrity of sensitive data and resources.

The implementation of a security policy to support the goals of the CIA triad might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer. However, each of these organizations, or any other organization (in any sector of the economy, whether profit-making or non-profit-making), should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage. An organization that develops security policies and uses framework-based security controls has a strong security posture.

As part of the process of adopting an effective organizational security posture, employees must be aware of their responsibilities. The structure of security responsibilities will depend on the size and hierarchy of an organization, but these roles are typical.

- Overall responsibility for the IT function lies with a **Chief Information Officer (CIO)**. This role might also have direct responsibility for security. Some organizations will also appoint a **Chief Technology Officer (CTO)**, with more specific responsibility for ensuring effective use of new and emerging IT products and solutions to achieve business goals.
- In larger organizations, internal responsibility for security might be allocated to a dedicated department, run by a **Chief Security Officer (CSO)** or Chief Information Security Officer (CISO).
- Managers may have responsibility for a domain, such as building control, web services, or accounting.

- Technical and specialist staff have responsibility for implementing, maintaining, and monitoring the policy. Security might be made of a core competency of systems and network administrators, or there may be dedicated security administrators. One such job title is **Information Systems Security Officer (ISSO)**.
- Nontechnical staff have the responsibility of complying with policy and with any relevant legislation.
- External responsibility for security (due care or liability) lies mainly with directors or owners, though again it is important to note that all employees share some measure of responsibility.

NIST's National Initiative for Cybersecurity Education (NICE) categorizes job tasks and job roles within the cybersecurity industry (gov/itl/applied-cybersecurity/nice/nice-framework-resource-center).

Information Security Competencies

IT professionals working in a role with security responsibilities must be competent in a wide range of disciplines, from network and application design to procurement and human resources (HR). The following activities might be typical of such a role:

- Participate in risk assessments and testing of security systems and make recommendations.
- Specify, source, install, and configure secure devices and software.
- Set up and maintain document access control and user privilege profiles.
- Monitor audit logs, review user privileges, and document access controls.
- Manage security-related incident response and reporting.
- Create and test business continuity and disaster recovery plans and procedures.
- Participate in security training and education programs.

Information Security Business Units

The following units are ofen used to represent the security function within the organizational hierarchy.

Security Operations Center (SOC)

A **security operations center (SOC)** is a location where security professionals monitor and protect critical information assets across other business functions, such as finance, operations, sales/marketing, and so on. Because SOCs can be difficult to establish, maintain, and finance, they are usually employed by larger corporations, like a government agency or a healthcare company.

A security operations center (SOC) provides resources and personnel to implement rapid incident detection and response, plus oversight of cybersecurity operations.
(Image © gorodenkoff 123RF.com.)

DevSecOps

Network operations and use of cloud computing make ever-increasing use of automation through software code. Traditionally, software code would be the responsibility of a programming or development team. Separate development and operations departments or teams can lead to silos, where each team does not work effectively with the other.

Development and operations (DevOps) is a cultural shift within an organization to encourage much more collaboration between developers and systems administrators. By creating a highly orchestrated environment, IT personnel and developers can build, test, and release software faster and more reliably. DevSecOps extends the boundary to security specialists and personnel, reflecting the principle that security is a primary consideration at every stage of software development and deployment. This is also known as shift left, meaning that security considerations need to be made during requirements and planning phases, not grafted on at the end. The principle of **DevSecOps** recognizes this and shows that security expertise must be embedded into any development project. Ancillary to this is the recognition that security operations can be conceived of as software development projects. Security tools can be automated through code. Consequently, security operations need to take on developer expertise to improve detection and monitoring.

Incident Response

A dedicated **computer incident response team (CIRT)**/computer security incident response team (CSIRT)/computer emergency response team (CERT) is a single point of contact for the notification of security incidents. This function might be handled by the SOC or it might be established as an independent business unit.

Review Activity:

Security Controls

Answer the following questions:

1. **You have implemented a secure web gateway that blocks access to a social networking site. How would you categorize this type of security control?**

2. **A company has installed motion-activated floodlighting on the grounds around its premises. What class and function is this security control?**

3. **A firewall appliance intercepts a packet that violates policy. It automatically updates its access control list to block all further packets from the source IP. What TWO functions did the security control perform?**

4. **If a security control is described as operational and compensating, what can you determine about its nature and function?**

5. **A multinational company manages a large amount of valuable intellectual property (IP) data, plus personal data for its customers and account holders. What type of business unit can be used to manage such important and complex security requirements?**

6. **A business is expanding rapidly, and the owner is worried about tensions between its established IT and programming divisions. What type of security business unit or function could help to resolve these issues?**

Lesson 1

Summary

You should be able to compare and contrast security controls using categories and functional types. You should also be able to explain how general security concepts and frameworks are used to develop and validate security policies and control selection.

Guidelines for Summarizing Security Concepts and Security Controls

Follow these guidelines when you assess the use of security controls and frameworks in your organization:

- Create a security mission statement and supporting policies that emphasize the importance of the CIA triad: confidentiality, integrity, availability.
- Assign roles so that security tasks and responsibilities are clearly understood and that impacts to security are assessed and mitigated across the organization.
- Consider creating business units, departments, or projects to support the security function, such as a SOC, CIRT, and DevSecOps.
- Identify and assess the laws and industry regulations that impose compliance requirements on your business.
- Select a framework that meets your organization's compliance requirements and business needs.
- Create a matrix of security controls that are currently in place to identify categories and functions—consider deploying additional controls for any unmatched capabilities.
- Perform a gap analysis to evaluate security capabilities against framework requirements and identify goals for developing additional cybersecurity competencies and improving overall information security assurance.