

CompTIA.



The Official CompTIA

Security+

Study Guide

Exam SY0-601



Official CompTIA Content Series for CompTIA Performance Certifications

**The Official
CompTIA
Security+
Study Guide
(Exam SY0-601)**

Acknowledgments



James Pengelly, Author

Thomas Reilly, Vice President, Learning

Katie Hoenicke, Director of Product Management

Evan Burns, Senior Manager, Learning Technology Operations and Implementation

James Chesterfield, Manager, Learning Content and Design

Becky Mann, Senior Manager, Product Development

Katherine Keyes, Content Specialist

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

CompTIA®, Security+®, and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright Notice

Copyright © 2020 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or visit <https://help.comptia.org>.

Table of Contents

Lesson 1: Comparing Security Roles and Security Controls.....	1
Topic 1A: Compare and Contrast Information Security Roles.....	2
Topic 1B: Compare and Contrast Security Control and Framework Types.....	8
Lesson 2: Explaining Threat Actors and Threat Intelligence	17
Topic 2A: Explain Threat Actor Types and Attack Vectors	18
Topic 2B: Explain Threat Intelligence Sources.....	25
Lesson 3: Performing Security Assessments	35
Topic 3A: Assess Organizational Security with Network Reconnaissance Tools.....	36
Topic 3B: Explain Security Concerns with General Vulnerability Types.....	50
Topic 3C: Summarize Vulnerability Scanning Techniques	57
Topic 3D: Explain Penetration Testing Concepts.....	67
Lesson 4: Identifying Social Engineering and Malware	73
Topic 4A: Compare and Contrast Social Engineering Techniques.....	74
Topic 4B: Analyze Indicators of Malware-Based Attacks	82
Lesson 5: Summarizing Basic Cryptographic Concepts	95
Topic 5A: Compare and Contrast Cryptographic Ciphers.....	96
Topic 5B: Summarize Cryptographic Modes of Operation	104
Topic 5C: Summarize Cryptographic Use Cases and Weaknesses.....	111
Topic 5D: Summarize Other Cryptographic Technologies.....	120
Lesson 6: Implementing Public Key Infrastructure	125
Topic 6A: Implement Certificates and Certificate Authorities.....	126
Topic 6B: Implement PKI Management.....	137

Lesson 7: Implementing Authentication Controls	147
Topic 7A: Summarize Authentication Design Concepts	148
Topic 7B: Implement Knowledge-Based Authentication.....	154
Topic 7C: Implement Authentication Technologies.....	164
Topic 7D: Summarize Biometrics Authentication Concepts	172
Lesson 8: Implementing Identity and Account Management Controls	179
Topic 8A: Implement Identity and Account Types	180
Topic 8B: Implement Account Policies	191
Topic 8C: Implement Authorization Solutions.....	199
Topic 8D: Explain the Importance of Personnel Policies	208
Lesson 9: Implementing Secure Network Designs	215
Topic 9A: Implement Secure Network Designs	216
Topic 9B: Implement Secure Switching and Routing	227
Topic 9C: Implement Secure Wireless Infrastructure.....	235
Topic 9D: Implement Load Balancers	247
Lesson 10: Implementing Network Security Appliances	255
Topic 10A: Implement Firewalls and Proxy Servers.....	256
Topic 10B: Implement Network Security Monitoring.....	268
Topic 10C: Summarize the Use of SIEM.....	275
Lesson 11: Implementing Secure Network Protocols	283
Topic 11A: Implement Secure Network Operations Protocols.....	284
Topic 11B: Implement Secure Application Protocols.....	292
Topic 11C: Implement Secure Remote Access Protocols.....	301
Lesson 12: Implementing Host Security Solutions	317
Topic 12A: Implement Secure Firmware	318
Topic 12B: Implement Endpoint Security	325
Topic 12C: Explain Embedded System Security Implications.....	331

Lesson 13: Implementing Secure Mobile Solutions	343
Topic 13A: Implement Mobile Device Management	344
Topic 13B: Implement Secure Mobile Device Connections	356
Lesson 14: Summarizing Secure Application Concepts	365
Topic 14A: Analyze Indicators of Application Attacks	366
Topic 14B: Analyze Indicators of Web Application Attacks.....	372
Topic 14C: Summarize Secure Coding Practices	383
Topic 14D: Implement Secure Script Environments	390
Topic 14E: Summarize Deployment and Automation Concepts.....	399
Lesson 15: Implementing Secure Cloud Solutions	407
Topic 15A: Summarize Secure Cloud and Virtualization Services	408
Topic 15B: Apply Cloud Security Solutions.....	418
Topic 15C: Summarize Infrastructure as Code Concepts	429
Lesson 16: Explaining Data Privacy and Protection Concepts.....	437
Topic 16A: Explain Privacy and Data Sensitivity Concepts.....	438
Topic 16B: Explain Privacy and Data Protection Controls.....	447
Lesson 17: Performing Incident Response	455
Topic 17A: Summarize Incident Response Procedures.....	456
Topic 17B: Utilize Appropriate Data Sources for Incident Response	465
Topic 17C: Apply Mitigation Controls.....	475
Lesson 18: Explaining Digital Forensics	483
Topic 18A: Explain Key Aspects of Digital Forensics Documentation	484
Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition	490
Lesson 19: Summarizing Risk Management Concepts	499
Topic 19A: Explain Risk Management Processes and Concepts	500
Topic 19B: Explain Business Impact Analysis Concepts.....	508

Lesson 20: Implementing Cybersecurity Resilience	515
Topic 20A: Implement Redundancy Strategies.....	516
Topic 20B: Implement Backup Strategies	522
Topic 20C: Implement Cybersecurity Resiliency Strategies	530
Lesson 21: Explaining Physical Security	539
Topic 21A: Explain the Importance of Physical Site Security Controls	540
Topic 21B: Explain the Importance of Physical Host Security Controls.....	548
Appendix A: Mapping Course Content to CompTIA Security+ (Exam SY0-601)	A-1
Solutions	S-1
Glossary.....	G-1
Index.....	I-1

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 and its industry-leading IT certifications are an important part of that mission. CompTIA's Security+ certification is a foundation-level certificate designed for IT administrators with two years' experience whose job role is focused on system security.

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to assist with cybersecurity duties in small and large organizations. These duties include assessments and monitoring; secure network, host, app, and cloud provisioning; data governance; and incident analysis and response.

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents—not just identify them.

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

comptia.org/certifications/security

Course Description

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-601) 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 computer 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:

- Compare security roles and security controls
- Explain threat actors and threat intelligence
- Perform security assessments and identify social engineering attacks and malware types
- Summarize basic cryptographic concepts and implement public key infrastructure
- Implement authentication controls
- Implement identity and account management controls
- Implement secure network designs, network security appliances, and secure network protocols
- Implement host, embedded/Internet of Things, and mobile security solutions
- Implement secure cloud solutions

- Explain data privacy and protection concepts
- Perform incident response and digital forensics
- Summarize risk management concepts and implement cybersecurity resilience
- Explain physical security

Target Student

The Official CompTIA Security+ Guide (Exam SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, devices, and data confidentiality/privacy in your organization. You can take this course to prepare for the CompTIA Security+ (Exam SY0-601) certification examination.

Prerequisites

- To ensure your success in this course, you should have basic Windows and Linux administrator skills and the ability to implement fundamental networking appliances and IP addressing concepts. CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are 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: 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 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.

Additional 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.

Student Icon	Student Icon Descriptive Text
	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 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

Comparing Security Roles and Security Controls

LESSON INTRODUCTION

Security is an ongoing process that includes assessing requirements, setting up organizational security systems, hardening them, monitoring them, responding to attacks in progress, and deterring attackers. As a security professional, it is important that you understand how the security function is implemented as departments or units and professional roles within different types of organizations. You must also be able to explain the importance of compliance factors and best practice frameworks in driving the selection of security controls.

Lesson Objectives

In this lesson, you will:

- Compare and contrast information security roles.
- Compare and contrast security control and framework types.

Topic 1A

Compare and Contrast Information Security Roles



EXAM OBJECTIVES COVERED

This topic provides background information about the role of security professionals and does not cover a specific exam objective.

To be successful and credible as a security professional, you should understand security in business starting from the ground up. You should also know the key security terms and ideas used by other security experts in technical documents and in trade publications. Security implementations are constructed from fundamental building blocks, just like a large building is constructed 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 (or 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, the way it is transferred, or the way it is 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 certain information should only be known to certain people.
- **Integrity** means that the data is stored and transferred as intended and that any modification is authorized.
- **Availability** means that information is accessible to those authorized to view or modify it.



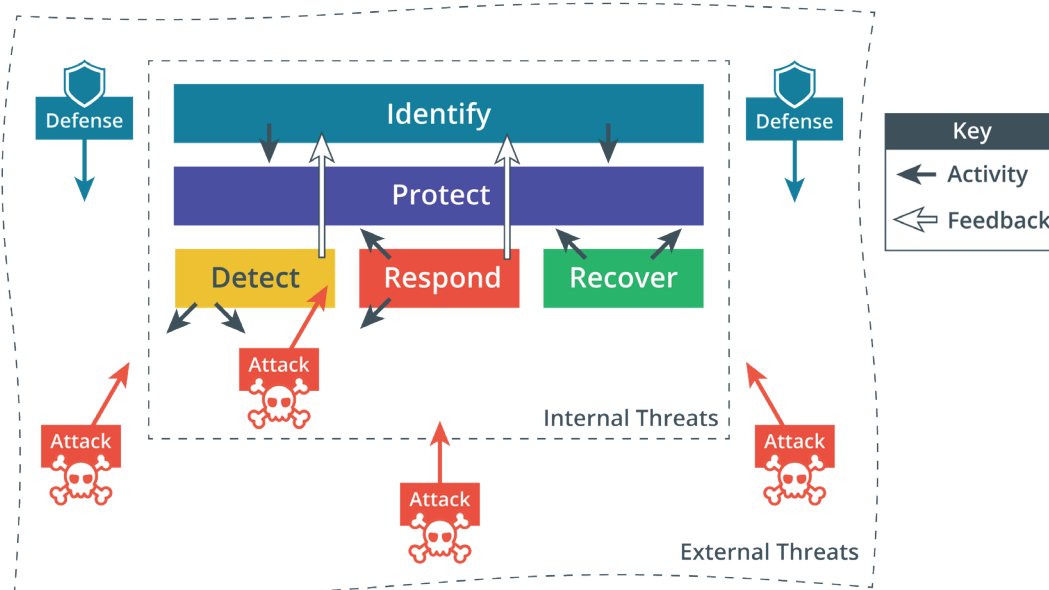
The triad can also be referred to as "AIC" to avoid confusion with the Central Intelligence Agency.

Some security models and researchers identify other properties that secure systems should exhibit. The most important of these is non-repudiation. **Non-repudiation** means that a subject 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 operations life cycle.
- 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.

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 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. It often consists of multiple individual policies. 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.

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 internal responsibility for security might be allocated to a dedicated department, run by a Director of Security, Chief Security Officer (CSO), or **Chief Information Security Officer (CISO)**. Historically, responsibility for security might have been allocated to an existing business unit, such as Information and Communications Technology (ICT) or accounting.

However, the goals of a network manager are not always well-aligned with the goals of security; network management focuses on availability over confidentiality. Consequently, security is increasingly thought of as a dedicated function or business unit with its own management structure.

- Managers may have responsibility for a domain, such as building control, ICT, or accounting.
- Technical and specialist staff have responsibility for implementing, maintaining, and monitoring the policy. Security might be made 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)**.
- Non-technical 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](https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center)).

Information Security Business Units

The following units are often 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 SOC's can be difficult to establish, maintain, and finance, they are usually employed by larger corporations, like a government agency or a healthcare company.



IBM Security Headquarters in Cambridge MA. (Image credit: John Mattern/Feature Photo Service for IBM.)

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 system administrators. By creating a highly orchestrated environment, IT personnel and developers can build, test, and release software faster and more reliably. Many consider a DevOps approach to administration as the only way organizations can take full advantage of the potential benefits offered by cloud service providers.

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 **cyber incident response team (CIRT)**/computer security incident response team (CSIRT)/computer emergency response team (CERT) as 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:

Information Security Roles

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 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?**
4. **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?**

Topic 1B

Compare and Contrast Security Control and Framework Types



EXAM OBJECTIVES COVERED

5.1 Compare and contrast various types of controls

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture

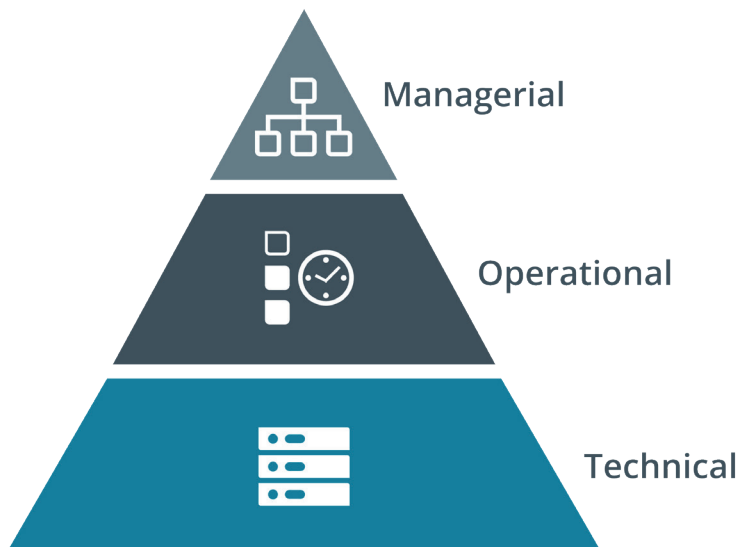
Information security and cybersecurity assurance is met by implementing security controls. As an information security professional, you must be able to compare types of security controls. You should also be able to describe how frameworks influence the selection and configuration of controls. By identifying basic security control types and how key frameworks and legislation drive compliance, you will be better prepared to select and implement the most appropriate controls for a given scenario.

Security Control Categories

Information and cybersecurity assurance is usually considered to take 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 should ideally be in place. Collectively, these procedures, activities, and tools can be referred to as security controls.

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

- **Technical**—the control is implemented as a system (hardware, software, or firmware). For example, firewalls, anti-virus software, and OS access control models are technical controls. Technical controls may also be described as logical controls.
- **Operational**—the control is implemented primarily by people rather than systems. For example, security guards and training programs are operational controls rather than technical controls.
- **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.



Categories of security controls.



Although it uses a more complex scheme, it is worth being aware of the way the National Institute of Standards and Technology (NIST) classifies security controls (nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).

Security Control Functional Types

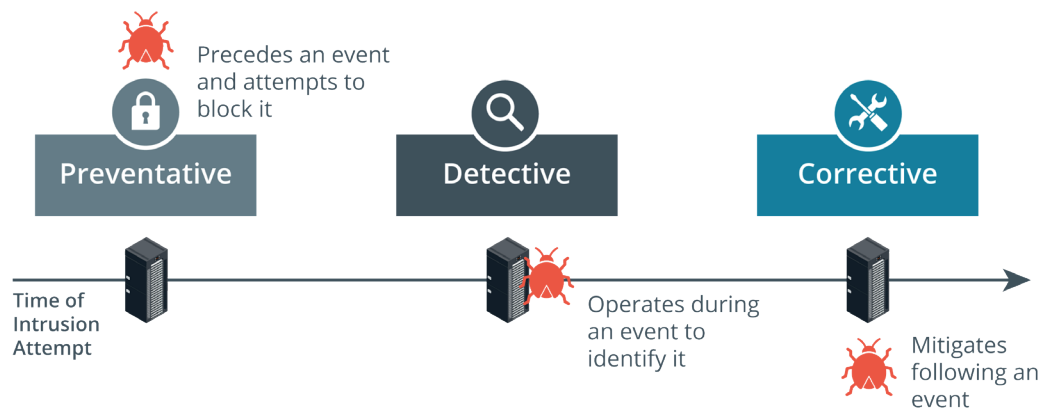
Security controls can also be classified in types according to the goal or function they perform:

- **Preventive**—the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventative control operates before an attack can take place. **Access control lists (ACL)** configured on firewalls and file system objects are preventative-type controls. Anti-malware software also acts as a preventative control, by blocking processes identified as malicious from executing. Directives and standard operating procedures (SOPs) can be thought of as administrative versions of preventative controls.
- **Detective**—the control may not prevent or deter access, but it will identify and record any attempted or successful intrusion. A detective control operates during the progress of an attack. Logs provide one of the best examples of detective-type controls.
- **Corrective**—the control acts to eliminate or reduce the impact of an intrusion event. A corrective control is used after an attack. A good example is a backup system that can restore data that was damaged during an intrusion. Another example is a patch management system that acts to eliminate the vulnerability exploited during the attack.

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

- **Physical**—Controls such as alarms, gateways, locks, lighting, security cameras, and guards that deter and detect access to premises and hardware are often classed separately.

- **Deterrent**—The control may not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion. This could include signs and warnings of legal penalties against trespass or intrusion.
- **Compensating**—The control serves as 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.



Other Control Functional Types:



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

NIST Cybersecurity Framework

A **cybersecurity framework (CSF)** is a list of activities and objectives undertaken to mitigate risks. 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 is valuable for giving a structure to internal risk management procedures and provides an externally verifiable statement of regulatory compliance. Frameworks are also 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.

There are many different frameworks, each of which categorize cybersecurity activities and controls in slightly different ways. These frameworks are non-regulatory in the sense that they do not attempt to address the specific regulations of a specific industry but represent "best practice" in IT security governance generally. Most organizations will have historically chosen a particular framework; some may use multiple frameworks in conjunction.

Most frameworks are developed for an international audience; others are focused on a domestic national audience. Most of the frameworks are associated with certification programs to show that staff and consultants can apply the methodologies successfully.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a relatively new addition to the IT governance space and distinct from other frameworks by focusing exclusively on IT security, rather than IT service provision more generally (nist.gov/cyberframework). It is developed for a US audience and focuses somewhat on US government, but its recommendations can be adapted for other countries and types of organizations.

NIST's Risk Management Framework (RMF) pre-dates the CSF. Where the CSF focuses on practical cybersecurity for businesses, the RMF is more prescriptive and principally intended for use by federal agencies (csrc.nist.gov/projects/risk-management/rmf-overview).

As well as its cybersecurity and risk frameworks, NIST is responsible for issuing the Federal Information Processing Standards (FIPS) plus advisory guides called Special Publications (csrc.nist.gov/publications/sp). Many of the standards and technologies covered in CompTIA Security+ are discussed in these documents.

ISO and Cloud Frameworks

International Organization for Standardization (ISO) 27K

The International Organization for Standardization (ISO) has produced a cybersecurity framework in conjunction with the International Electrotechnical Commission (IEC). The framework was established in 2005 and revised in 2013. Unlike the NIST framework, the ISO 27001 Information Security Management standard must be purchased (iso.org/standard/54534.html). **ISO 27001** is part of an overall 27000 series of information security standards, also known as 27K. Of these, 27002 classifies security controls, 27017 and 27018 reference cloud security, and 27701 focuses on personal data and privacy.

ISO 31K

Where ISO 21K is a cybersecurity framework, **ISO 31K** (iso.org/iso-31000-risk-management.html) is an overall framework for enterprise risk management (ERM). ERM considers risks and opportunities beyond cybersecurity by including financial, customer service, competition, and legal liability factors. ISO 31K establishes best practices for performing risk assessments.

Cloud Security Alliance

The not-for-profit organization **Cloud Security Alliance (CSA)** produces various resources to assist cloud service providers (CSP) in setting up and delivering secure cloud platforms. These resources can also be useful for cloud consumers in evaluating and selecting cloud services.

- Security Guidance (cloudsecurityalliance.org/research/guidance)—a best practice summary analyzing the unique challenges of cloud environments and how on-premises controls can be adapted to them.
- Enterprise reference architecture (ea.cloudsecurityalliance.org)—best practice methodology and tools for CSPs to use in architecting cloud solutions. The solutions are divided across a number of domains, such as risk management and infrastructure, application, and presentation services.
- Cloud controls matrix (cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix)—lists specific controls and assessment guidelines that should be implemented by CSPs. For cloud consumers, the matrix acts as a starting point for cloud contracts and agreements as it provides a baseline level of security competency that the CSP should meet.

Statements on Standards for Attestation Engagements (SSAE) Service Organization Control (SOC)

The **Statements on Standards for Attestation Engagements (SSAE)** are audit specifications developed by the American Institute of Certified Public Accountants

(AICPA). These audits are designed to assure consumers that service providers— notably cloud providers, but including any type of hosted or third-party service— meet professional standards (aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html). Within SSAE No. 18 (the current specification), there are several levels of reporting:

- Service Organization Control (SOC2)— evaluates the internal controls implemented by the service provider to ensure compliance with Trust Services Criteria (TSC) when storing and processing customer data. TSC refers to security, confidentiality, integrity, availability, and privacy properties. An SOC2 Type I report assesses the system design, while a Type II report assesses the ongoing effectiveness of the security architecture over a period of 6-12 months. SOC2 reports are highly detailed and designed to be restricted. They should only be shared with the auditor and regulators and with important partners under non disclosure agreement (NDA) terms.
- SOC3—a less detailed report certifying compliance with SOC2. SOC3 reports can be freely distributed.

Benchmarks and Secure Configuration Guides

Although a framework gives a "high-level" view of how to plan IT services, it does not generally provide detailed implementation guidance. At a system level, the deployment of servers and applications is covered by benchmarks and secure configuration guides.

Center for Internet Security (CIS)

The **Center for Internet Security** (cisecurity.org) is a not-for-profit organization (founded partly by The SANS Institute). It publishes the well-known "The 20 CIS Controls." The CIS-RAM (Risk Assessment Method) can be used to perform an overall evaluation of security posture (learn.cisecurity.org/cis-ram).

CIS also produces **benchmarks** for different aspects of cybersecurity. For example, there are benchmarks for compliance with IT frameworks and compliance programs, such as **PCI DSS**, NIST 800-53, SOX, and ISO 27000. There are also product-focused benchmarks, such as for Windows Desktop, Windows Server, macOS, Linux, Cisco, web browsers, web servers, database and email servers, and VMware ESXi. The CIS-CAT (Configuration Access Tool) can be used with automated vulnerability scanners to test compliance against these benchmarks (cisecurity.org/cybersecurity-tools/cis-cat-pro/cis-cat-faq).

OS/Network Appliance Platform/Vendor-specific Guides

Operating system (OS) best practice configuration lists the settings and controls that should be applied for a computing platform to work in a defined roles, such as client workstation, authentication server, network switch/router/firewall, web/application server, and so on.

Most vendors will provide guides, templates, and tools for configuring and validating the deployment of network appliances, operating systems, web servers, and application/database servers. The security configurations for each of these devices will vary not only by vendor but by device and version as well. The vendor's support portal will host the configuration guides (along with setup/install guides and software downloads and updates) or they can be easily located using a web search engine.

There is also detailed guidance available from several organizations to cover both vendor-neutral deployments and to provide third-party assessment and advice on deploying vendor products. Apart from the CIS controls, some notable sources include:

- Department of Defense Cyber Exchange provides Security Technical Implementation Guides (STIGs) with hardening guidelines for a variety of software and hardware solutions (public.cyber.mil).

- National Checklist Program (NCP) by NIST provides checklists and benchmarks for a variety of operating systems and applications (nvd.nist.gov/ncp/repository).

Application Servers

Most application architectures use a client/server model. This means that part of the application is a client software program, installed and run on separate hardware to the server application code. The client interacts with the server over a network. Attacks can therefore be directed at the local client code, at the server application, or at the network channel between them. As well as coding issues, the applications need to take account of platform issues. The client application might be running in a computing host alongside other, potentially malicious, software. Code that runs on the client should not be trusted. The server-side code should implement routines to verify that input conforms to what is expected.

Web Server Applications

A web application is a particular type of client/server architecture. A web application leverages existing technologies to simplify development. The application uses a generic client (a web browser), and standard network protocols and servers (HTTP/HTTPS). The specific features of the application are developed using code running on the clients and servers. Web applications are also likely to use a multi-tier architecture, where the server part is split between application logic and data storage and retrieval. Modern web applications may use even more distributed architectures, such as microservices and serverless.

The **Open Web Application Security Project (OWASP)** is a not-for-profit, online community that publishes several secure application development resources, such as the Top 10 list of the most critical application security risks (owasp.org/www-project-top-ten). OWASP has also developed resources, such as the Zed Attack Proxy and Juice Shop (a deliberately unsecure web application), to help investigate and understand penetration testing and application security issues.

Regulations, Standards, and Legislation

The key frameworks, benchmarks, and configuration guides may be used to demonstrate compliance with a country's legal/regulatory requirements or with industry-specific regulations. *Due diligence* is a legal term meaning that responsible persons have not been negligent in discharging their duties. Negligence may create criminal and civil liabilities. Many countries have enacted legislation that criminalizes negligence in information management. In the US, for example, the **Sarbanes-Oxley Act (SOX)** mandates the implementation of risk assessments, internal controls, and audit procedures. The Computer Security Act (1987) requires federal agencies to develop security policies for computer systems that process confidential information. In 2002, the Federal Information Security Management Act (FISMA) was introduced to govern the security of data processed by federal government agencies.



Some regulations have specific cybersecurity control requirements; others simply mandate "best practice," as represented by a particular industry or international framework. It may be necessary to perform mapping between different industry frameworks, such as NIST and ISO 27K, if a regulator specifies the use of one but not another. Conversely, the use of frameworks may not be mandated as such, but auditors are likely to expect them to be in place as a demonstration of a strong and competent security program.

Personal Data and the General Data Protection Regulation (GDPR)

Where some types of legislation address cybersecurity due diligence, others focus in whole or in part on information security as it affects privacy or personal data. Privacy

is a distinct concept from security. Privacy requires that collection and processing of personal information be both secure and fair. Fairness and the right to privacy, as enacted by regulations such as the European Union's **General Data Protection Regulation (GDPR)**, means that personal data cannot be collected, processed, or retained without the individual's informed consent. *Informed consent* means that the data must be collected and processed only for the stated purpose, and that purpose must be clearly described to the user in plain language, not legalese. GDPR (ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr) gives data subjects rights to withdraw consent, and to inspect, amend, or erase data held about them.

National, Territory, or State Laws

Compliance issues are complicated by the fact that laws derive from different sources. For example, the GDPR does not apply to American data subjects, but it does apply to American companies that collect or process the personal data of people in EU countries. In the US, there are national federal laws, state laws, plus a body of law applying to US territories (Puerto Rico, the US Virgin Islands, Guam, and American Samoa). Federal laws tend to focus either on regulations like FISMA for federal departments or as "vertical" laws affecting a particular industry. Examples of the latter include the **Gramm-Leach-Bliley Act (GLBA)** for financial services, and the Health Insurance Portability and Accountability Act (HIPAA).

Some states have started to introduce "horizontal" personal data regulations, similar to the approach taken by the GDPR. One high-profile example of state legislation is the California Consumer Privacy Act (CCPA) (csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html).



Varonis' blog contains a useful overview of privacy laws in the US (varonis.com/blog/us-privacy-laws).

Payment Card Industry Data Security Standard (PCI DSS)

Compliance issues can also arise from industry-mandated regulations. For example, the Payment Card Industry Data Security Standard (PCI DSS) defines the safe handling and storage of financial information (pcisecuritystandards.org/pci_security).

Review Activity:

Security Control and Framework Types

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 is the security control performing?**
4. **If a security control is described as operational and compensating, what can you determine about its nature and function?**
5. **If a company wants to ensure it is following best practice in choosing security controls, what type of resource would provide guidance?**

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 regulations, frameworks, and benchmarks are used to develop and validate security policies and control selection.

Guidelines for Comparing Security Roles and Security Controls

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

- Create a security mission statement and supporting policies that emphasizes 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, CSIRT, and DevSecOps.
- Identify and assess the laws and industry regulations that impose compliance requirements on your business.
- Select a framework that meets 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.
- Use benchmarks, secure configuration guides, and development best practices as baselines for deploying assets.
- Evaluate security capabilities against framework tiers and identify goals for developing additional cybersecurity competencies and improving overall information security assurance.