**Security Frameworks and Their Role in Protecting Organizations**

Organizations establish **security plans** to defend against **threats, risks, and vulnerabilities**. However, many security requirements **overlap**, which is why organizations rely on **security frameworks** to develop **custom policies and procedures**.

**What Are Security Frameworks?**

Security frameworks are **guidelines** designed to help organizations **mitigate risks** and **protect data and privacy** from threats like **social engineering attacks** and **ransomware**.

Security isn't just about **cybersecurity**—it also includes **physical security** measures. For example:

* Employees may need a **key card or badge** to access a building.
* Organizations may implement **security cameras and visitor logs** to prevent unauthorized access.

Some frameworks also provide guidance on **preventing, detecting, and responding** to security breaches. This is critical for defending against **phishing attacks** and other forms of **social engineering** that **target employees**.

**The Role of Employees in Security**

Since **people are the biggest security threat**, frameworks help organizations create:

* **Training programs** to educate employees on recognizing **security threats and red flags**.
* **Incident response plans** to ensure employees can quickly **report and address security concerns**.

**The Analyst’s Role**

As an **entry-level security analyst**, your job will involve:

* Understanding and **following security frameworks** in your organization.
* Implementing security plans to **protect employees and sensitive data**.
* Educating staff on **best practices** to defend against **social engineering attacks, breaches, and other security incidents**.

### ****Understanding Security Controls****

While **frameworks** provide a broad **security strategy** for managing risks, **security controls** are specific measures designed to **reduce and mitigate** these risks. Without proper security controls, organizations may suffer **financial losses, reputational damage, and exposure to security risks** such as **trespassing, fake employee accounts, or unauthorized benefits**.

### ****What Are Security Controls?****

**Security controls** are **safeguards** that reduce specific security risks. Let’s explore three **common types** of security controls:

#### **1. Encryption**

Encryption is the process of **converting data from a readable format (plaintext) into an encoded format (ciphertext)**.

* **Ciphertext** is unreadable until decrypted back into plaintext.
* **Purpose:** Ensures **confidentiality** of sensitive data, such as **customer account details** and **Social Security numbers**.

#### **2. Authentication**

Authentication is the process of **verifying the identity of a user or system**.

* A common example is **logging into a website with a username and password**.
* **Multi-factor authentication (MFA)** adds an extra layer of security by requiring **a password plus another factor** (e.g., a security code, fingerprint, or facial recognition).
* **Biometrics** (fingerprints, eye scans, or palm scans) are also used for authentication.

One potential **social engineering attack** that can exploit **biometric authentication** is **vishing** (voice phishing).

* **Vishing** is when attackers use **voice manipulation** to impersonate someone and gain unauthorized access to sensitive data.

#### **3. Authorization**

Authorization determines **what resources a person or system is allowed to access**.

* Even if a user is **authenticated**, they may not have **authorization** to access certain information.
* Example: A **federal employee** may have authorization to access **deep web data** that is restricted to the general public.

### ****The Bigger Picture: The CIA Triad****

The **security controls** discussed here are **fundamental components** of the **CIA triad**—a core model used by security teams to **protect organizations**.

Up next, we’ll explore the **CIA triad** and how it serves as a foundation for security professionals in safeguarding critical assets.

# The relationship between frameworks and controls

Previously, you learned how organizations use security frameworks and controls to protect against threats, risks, and vulnerabilities. This included discussions about the National Institute of Standards and Technology’s (NIST’s) Risk Management Framework (RMF) and Cybersecurity Framework (CSF), as well as the confidentiality, integrity, and availability (CIA) triad. In this reading, you will further explore security frameworks and controls and how they are used together to help mitigate organizational risk.

## Frameworks and controls

**Security frameworks** are guidelines used for building plans to help mitigate risk and threats to data and privacy. Frameworks support organizations’ ability to adhere to compliance laws and regulations. For example, the healthcare industry uses frameworks to comply with the United States’ Health Insurance Portability and Accountability Act (HIPAA), which requires that medical professionals keep patient information safe.

**Security controls** are safeguards designed to reduce specific security risks. Security controls are the measures organizations use to lower risk and threats to data and privacy. For example, a control that can be used alongside frameworks to ensure a hospital remains compliant with HIPAA is requiring that patients use multi-factor authentication (MFA) to access their medical records. Using a measure like MFA to validate someone’s identity is one way to help mitigate potential risks and threats to private data.

## Specific frameworks and controls

There are many different frameworks and controls that organizations can use to remain compliant with regulations and achieve their security goals. Frameworks covered in this reading are the Cyber Threat Framework (CTF) and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001. Several common security controls, used alongside these types of frameworks, are also explained.

### ****Cyber Threat Framework (CTF)****

According to the Office of the Director of National Intelligence, the CTF was developed by the U.S. government to provide “a common language for describing and communicating information about cyber threat activity.” By providing a common language to communicate information about threat activity, the CTF helps cybersecurity professionals analyze and share information more efficiently. This allows organizations to improve their response to the constantly evolving cybersecurity landscape and threat actors' many tactics and techniques.

### ****International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001****

An internationally recognized and used framework is ISO/IEC 27001. The ISO 27000 family of standards enables organizations of all sectors and sizes to manage the security of assets, such as financial information, intellectual property, employee data, and information entrusted to third parties. This framework outlines requirements for an information security management system, best practices, and controls that support an organization’s ability to manage risks. Although the ISO/IEC 27001 framework does not require the use of specific controls, it does provide a collection of controls that organizations can use to improve their security posture.

### ****Controls****

Controls are used alongside frameworks to reduce the possibility and impact of a security threat, risk, or vulnerability. Controls can be physical, technical, and administrative and are typically used to prevent, detect, or correct security issues.

Examples of physical controls:

* Gates, fences, and locks
* Security guards
* Closed-circuit television (CCTV), surveillance cameras, and motion detectors
* Access cards or badges to enter office spaces

Examples of technical controls:

* Firewalls
* MFA
* Antivirus software

Examples of administrative controls:

* Separation of duties
* Authorization
* Asset classification

To learn more about controls, particularly those used to protect health-related assets from a variety of threat types, review the U.S. Department of Health and Human Services’ [Physical Access Control presentation](https://www.hhs.gov/sites/default/files/physical-access-control.pdf)

.

## Key takeaways

Cybersecurity frameworks and controls are used together to establish an organization’s security posture. They also support an organization’s ability to meet security goals and comply with laws and regulations. Although these frameworks and controls are typically voluntary, organizations are strongly encouraged to implement and use them to help ensure the safety of critical assets.