more about framework and controls

Welcome to week 2

Welcome back! As a security analyst, your job isn't just keeping organization safe. Your role is much more important. You're also helping to keep people safe. Breaches that affect customers', vendors', and employees' data can cause significant damage to people's financial stability and their reputations. As an analyst, your day-to-day work will help keep people and organizations safe.

In this section of the course, we'll discuss security frameworks, controls, and design principles in more detail, and how they can be applied to security audits to help protect organizations and people.

Keeping customer information confidential is a crucial part of my daily work at Google. The NIST Cybersecurity Framework plays a large part in this. The framework ensures the protection and compliance of customer tools and personal work devices through the use of security controls.

Welcome to the world of security frameworks and controls. Let's get started!

Frameworks

In an organization, plans are put in place to protect against a variety of threats, risks, and vulnerabilities. However, the requirements used to protect organizations and people often overlap. Because of this, organizations use security frameworks as a starting point to create their own security policies and processes.

Let's start by quickly reviewing what frameworks are. Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy, such as social engineering attacks and ransomware. Security involves more than just the virtual space. It also includes the physical, which is why many organizations have plans to maintain safety in the work environment. For example, access to a building may require using a key card or badge.

Other security frameworks provide guidance for how to prevent, detect, and respond to security breaches. This is particularly important when trying to protect an organization from social engineering attacks like phishing that target their employees.

Remember, people are the biggest threat to security. So frameworks can be used to create plans that increase employee awareness and educate them about how they can protect the organization, their co-workers, and themselves. Educating employees about existing security challenges is essential for minimizing the possibility of a breach.

Providing employee training about how to recognize red flags, or potential threats, is essential, along with having plans in place to quickly report and address security issues. As an analyst, it will be important for you to understand and implement the plans your organization has in place to keep the organization, its employees, and the people it serves safe from social engineering attacks, breaches, and other harmful security incidents.

Coming up, we'll review and discuss security controls, which are used alongside frameworks to achieve an organization's security goals.

Controls

While frameworks are used to create plans to address security risks, threats, and vulnerabilities, controls are used to reduce specific risks. If proper controls are not in place, an organization could face significant financial impacts and damage to their reputation because of exposure to risks including trespassing, creating fake employee accounts, or providing free benefits.

Let's review the definition of controls. Security controls are safeguards designed to reduce specific security risks. In this video, we'll discuss three common types of controls: encryption, authentication, and authorization.

Encryption is the process of converting data from a readable format to an encoded format. Typically, encryption involves converting data from plaintext to ciphertext. Ciphertext is the raw, encoded message that's unreadable to humans and computers. Ciphertext data cannot be read until it's been decrypted into its original plaintext form. Encryption is used to ensure confidentiality of sensitive data, such as customers' account information or social security numbers.

Another control that can be used to protect sensitive data is authentication. Authentication is the process of verifying who someone or something is. A real-world example of authentication is logging into a website with your username and password. This basic form of authentication proves that you know the username and password and should be allowed to access the website. More advanced methods of authentication, such as multi-factor authentication, or MFA, challenge the user to demonstrate that they are who they claim to be by requiring both a password and an additional form of authentication, like a security code or biometrics, such as a fingerprint, voice, or face scan.

Biometrics are unique physical characteristics that can be used to verify a person's identity. Examples of biometrics are a fingerprint, an eye scan, or a palm scan. One example of a social engineering attack that can exploit biometrics is vishing. Vishing is the exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source. For example, vishing could be used to impersonate a person's voice to steal their identity and then commit a crime.

Another very important security control is authorization. Authorization refers to the concept of granting access to specific resources within a system. Essentially, authorization is used to verify that a person has permission to access a resource. As an example, if you're working as an entry-level security analyst for the federal government, you could have permission to access data through the deep web or other internal data that is only accessible if you're a federal employee.

The security controls we discussed today are only one element of a core security model known as the CIA triad. Coming up, we'll talk more about this model and how security teams use it to protect their organizations.

The relationship between frameworks and controls

Previously, you learned how organizations use security frameworks and controles to protect againced threads, risks, and vulnerabilities. This inclueds 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, avalability (CIA) triad. in this reading, you will further explore security frameworks, and controls and how they are used together to help mitigate organizational risk

Framework 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 Portability9 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 framework and corntrols

There are many different frameworks and controls that organizations can use to remain complient with regulations and achive their security goals. Frameworks covered in this reading are Cyber Threat Framework (CTF) and hte International Organizations for Standaridization/International Electronics Commisions (ISO/IEC) 27001. Several common security controls, used alongiside 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.

Controles
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.

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.