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.

Revision #4
Created 2023-06-05 16:49:03 UTC by naruzkurai
Updated 2023-06-05 20:15:24 UTC by naruzkurai