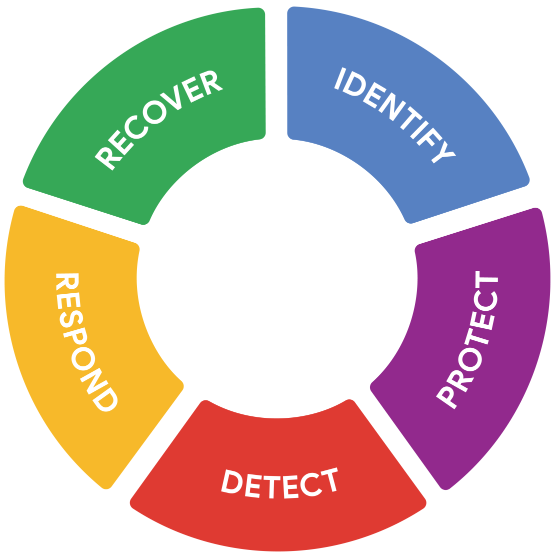
Security guidelines in action

Organizations often face an overwhelming amount of risk. Developing a security plan from the beginning that addresses all risk can be challenging. This makes security frameworks a useful option.

Previously, you learned about the NIST Cybersecurity Framework (CSF). A major benefit of the CSF is that it's flexible and can be applied to any industry. In this reading, you'll explore how the NIST CSF can be implemented.



Origins of the framework

Originally released in 2014, NIST developed the Cybersecurity Framework to protect critical infrastructure in the United States. NIST was selected to develop the CSF because they are an unbiased source of scientific data and practices. NIST eventually adapted the CSF to fit the needs of businesses in the public and private sector. Their goal was to make the framework more flexible, making it easier to adopt for small businesses or anyone else that might lack the resources to develop their own security plans.

Implementing the CSF

Since its creation, many businesses have used the NIST CSF. As you might recall, the framework consists of three main components:

- Core
- Tiers
- Profiles

These three components were designed to help any business improve their security operations. Although there are only three components, the entire framework consists of a complex system of subcategories and processes.

CSF can be a challenge to implement due to its high level of detail. It can also be tough to find where the framework fits in. For example, some businesses have established security plans, making it unclear how CSF can benefit them. Alternatively, some businesses might be in the early stages of building their plans and need a place to start.

In any scenario, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides detailed guidance that any organization can use to implement the CSF. This is a quick overview and summary of their recommendations:

- **Create a current profile** of the security operations and outline the specific needs of your business.
- **Perform a risk assessment** to identify which of your current operations are meeting business and regulatory standards.
- **Analyze and prioritize existing gaps** in security operations that place the businesses assets at risk.
- **Implement a plan of action** to achieve your organization's goals and objectives.

Pro tip: Always consider current risk, threat, and vulnerability trends when using the NIST CSF.

You can learn more about implementing the CSF in this report by CISA that outlines how the framework was applied in the commercial facilities sector.

Industries embracing the CSF

The NIST CSF has continued to evolve since its introduction in 2014. Its design is influenced by the standards and best practices of some of the largest companies in the world.

A benefit of the framework is that it aligns with the security practices of many organizations across the global economy. It also helps with regulatory compliance that might be shared by business partners.

Key takeaways

The NIST CSF is designed to be a flexible guide for organizations to assess and improve their security practices. It is a useful framework that combines the security best practices of industries around the world. Implementing the CSF can be a challenge for any organization. The CSF can help business meet regulatory compliance requirements to avoid financial and reputational risks.

Mark as completed