Google Cloud

# Controls that contribute to security depth

So far, you've learned that implementing controls is an important aspect to helping strengthen security posture. Controls are safeguards designed to reduce specific security risks. They also contribute to a defense in depth architecture where each control plays a pivotal role in defending cloud assets. Using frameworks, like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) alongside controls, can help organizations achieve improved security posture.

In this reading, you'll learn more about security controls and practices, and explore examples of how to implement them. Please note that this should not be considered legal advice.

## Security controls

Many organizations use established frameworks as a guide to implement security controls. For example, organizations using Google Cloud can use the NIST CSF as a guide to incorporate best practices and controls into their cloud environment. The NIST CSF framework recommends using controls in these categories to help strengthen security in a cloud environment:

- Identify
- Protect
- Detect
- Respond
- Recover

### Identify

The identify category highlights the importance of understanding an organization's critical assets and systems, along with their associated risks. Risks include anything that can impact the confidentiality, integrity, or availability of an asset. Organizations catalog their assets, like computers and other physical devices, data, and personally identifiable information. Then, they rank the severity of risks to each asset type, and identify gaps where security controls are necessary or need strengthening.

### Protect

Protective controls shield cloud resources. There are several ways to implement this control type. For example, only authorized users should have access to the CSP's hardware and software. This helps protect the provider's physical devices and the software that runs on them. Another example of employing protective controls is establishing network integrity, like using firewalls and network segmentation. Protecting the network is crucial to safeguarding against various cyber attacks. Also, organizations should provide training to employees that raises awareness about potential cyber threats and provides information about how to prevent them.

### Detect

Detective controls identify potential threats and events. Both physical and network environments should be monitored to alert for suspicious activities. Intrusion detection systems are commonly used to monitor and detect potential threats. Organizations can also use tools to detect phishing, malware, insecure libraries, and other threats and vulnerabilities. When a threat is discovered, it should be analyzed to discover more about the methods used to conduct the attack.

### Respond

Responsive controls involve many components, ranging from planning, to improving processes in the event of attacks, to disaster recovery. Responsive controls leverage automation in tools and applications to respond to detected security events or incidents. Once detective controls provide real-time alerts, and notify teams of security events, automated tools can help contain and mitigate incidents. Then, security teams can act on established processes that outline how to react in the event of incidents.

### Recover

Recovery controls are important to restore access and performance when failures occur. Ensuring resources have high availability is one component that helps facilitate recovery. Replicating resources across zones and regions helps organizations restore assets quickly. Another control includes maintaining backup systems that can deploy in case of an attack.

## Key takeaways

Security controls are an essential part of a defense in depth strategy. Using frameworks is one way to incorporate controls that help identify, protect, detect, respond, and recover cloud assets. As a cloud security professional, you'll use these types of controls as a regular part of your job.

## Resources for more information

The following resource provides more information about security controls:

- Best practices for applying the NIST CSF on Google Cloud