Google Cloud

Learn more about security controls

Previously, you learned that a security control is a measure used to manage risks. You also learned that compliance is evidence that an organization has met required laws, regulations, and standards. Technology is always changing and advancing, and so are the standards, laws, and regulations created to reduce risk in cloud environments. Now more than ever, it's important to know about the different groups of controls that can help meet compliance obligations and manage risk.

In this reading, you'll explore the different groups of controls called control families outlined by the National Institute of Standards and Technology (NIST 800-53). Please note, the following reading should not be considered legal advice.

NIST CSF and NIST Special Publication 800-53

The NIST CSF provides a flexible framework that organizations can use for creating and maintaining an information security program. It includes several core pillars, including: Identify, Protect, Detect, Respond, and Recover. The NIST CSF also offers a broad cybersecurity structure.

The NIST Special Publication (SP) 800-53 is a set of recommended security and privacy controls to help organizations meet compliance requirements. The NIST SP 800-53 provides security controls for implementing the NIST CSF. It also provides more specific security control guidance, especially for FedRAMP compliance than the NIST CSF does.

The NIST SP 800-53 provides a set of over 1,000 controls, separated into 20 groups called families, that support the development of secure information systems. Control families are important because they represent similar types of controls to help address a set of threats. For example, the incident response family provides examples of controls to help organizations respond to an incident, and aid in recovery. These families help cybersecurity professionals by providing a clear way to organize and categorize the many different controls in the NIST SP 800-53.

NIST SP 800-53 control families

NIST SP 800-53 contains 20 different control families. Each family is its own separate category or area of focus. There are more than 1,000 total controls represented within these families.

Access control (AC)

The access control (AC) control family includes controls that determine who has access to assets. These assets include account management, system privileges, and remote access. AC controls can also help manage the level of user access, including when users can access the system.

Audit and accountability (AU)

The audit and accountability (AU) control family includes security controls related to an organization's audit capabilities. This includes audit policies and procedures, audit logging, audit report generation, and protection of audit information.

Awareness and training (AT)

The awareness and training (AT) control family includes security training and procedures that are unique to an organization. The main focus of this family is to keep employee cybersecurity education a priority.

Configuration management (CM)

Controls in the configuration management (CM) control family are preventive controls specific to an organization's configuration management policies. These types of controls help to manage, assess, and improve the configuration of software and systems.

Contingency planning (CP)

Controls in the contingency planning (CP) control family include controls for an organization's contingency plan for a cybersecurity event. This includes contingency plan testing, updating, training, backups, and system reconstitution.

Identification and authentication (IA)

Controls in the identification and authentication (IA) control family include the identification and authentication of organizational and non-organizational users. These controls ensure that the identification and authentication policies in an organization are met.

Incident response (IR)

Controls in the incident response (IR) control family ensure that specific incident response policies and procedures are followed. This includes incident response training, testing, monitoring, reporting, and response plan.

Maintenance (MA)

Controls in the maintenance (MA) control family cover system maintenance, software updates, inspection procedures, and logging tools.

Media protection (MP)

Controls in the media protection (MP) control family include controls specific to access, marking, storage, transport policies, sanitization, and defined organizational media use.

Personnel Security (PS)

Controls in the personnel security (PS) control family relate to how an organization protects its personnel. These controls include personnel screening, termination, transfers, sanctions, and access agreements.

Physical and Environmental Protection (PE)

Controls in the physical and environmental protection (PE) control family are implemented to protect systems, buildings, and supporting infrastructure against physical threats. These controls include physical access authorizations, monitoring, visitor records, emergency shutoff, power, lighting, fire protection, and water damage protection.

Planning (PL)

Controls in the planning (PL) control family relate to security planning policies, and include system architecture, system security plans, privacy security plans, and management processes.

Program Management (PM)

Controls in the program management (PM) control family focus on cybersecurity program management and operations. These controls include things like plan of action processes, risk management strategy, and cloud architecture.

Risk Assessment (RA)

Controls in the risk assessment (RA) control family relate to an organization's risk assessment policies and vulnerability scanning capabilities.

Security Assessment and Authorization (SA)

Controls in the security assessment and authorization (SA) control family include supplemental security assessments, authorizations, continuous monitoring, and plans of action.

System and communications protection (SC)

Controls in the system and communications protection(SC) control family are responsible for systems and communications protection procedures, including boundary protection, protection of information at rest, collaborative computing devices, cryptographic protection, and denial of service protection.

System and information integrity (SI)

To protect systems and information integrity, use controls in the system and information integrity (SI) control family. This control family involves flaw remediation, malicious code protection, information system monitoring, security alerts, software, firmware integrity, and spam protection.

System and services acquisition (SA)

Controls in the system and services acquisition(SA) control family include information system documentation controls, development configuration management controls, and developer security testing and evaluation controls.

Key takeaways

Security controls are a key part of meeting compliance obligations and managing risk. There are many possibilities when it comes to controls, so knowing control families laid out by NIST SP 800-53 can be a useful resource when selecting controls for risk management and compliance. These control families are related to specific types of threats and the strategies used to mitigate them. Understanding and using these resources will help you reduce risk and secure your assets in the cloud.

Resources for more information

Review these resources for more information about the NIST SP 800-53 controls:

- This page provides information on resources for control implementers for NIST SP 800-53
- The NIST SP 800-53 Control Catalog provides a control catalog that lists all controls included in NIST SP 800-53 by family
- This document provides an example control map for NIST SP 800-53: NIST SP 800-53 Control Map