Google Cloud

Risk management and security frameworks

You've learned that a risk management framework is a set of practices, processes, and technologies that enable an organization to identify, assess, analyze, and manage risk within an organization. You've also been introduced to some of the most common risk management frameworks. Frameworks are a tool that organizations can use to achieve a better defense and meet compliance regulations. Frameworks can do this by providing security guidelines and best practices, recommending security controls, or both. Cloud security analysts use these frameworks to help strengthen their organization's security posture.

In this reading, you'll learn more details about cybersecurity frameworks and the management of security risks. Please note, the following reading should not be considered legal advice.

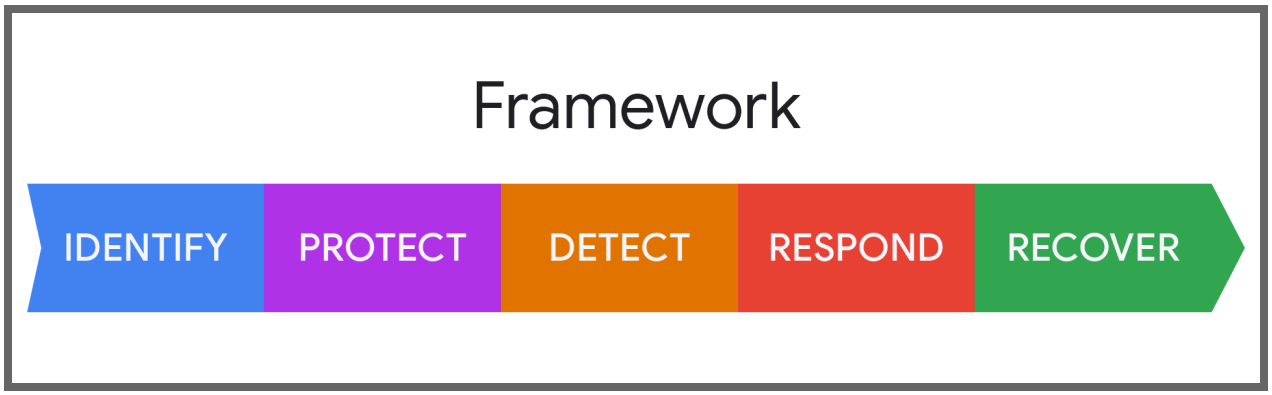
NIST Cybersecurity Framework (CSF)

The NIST CSF is designed to act as a translation layer to enable communication between multidisciplinary teams. It consists of three main parts that include:

- The Framework Core
- Profiles
- Implementation Tiers

The Framework Core

The framework core contains five functions: identify, protect, detect, respond, and recover. These functions are designed to create communication about cybersecurity between cybersecurity professionals and other organizational stakeholders. The framework core aims to make cyber risk a part of the overall risk management strategy for an organization. The CSF does not require specific controls. Instead, each of the framework functions has a series of categories, subcategories, and references so that organizations can implement the appropriate controls to improve their cybersecurity posture.



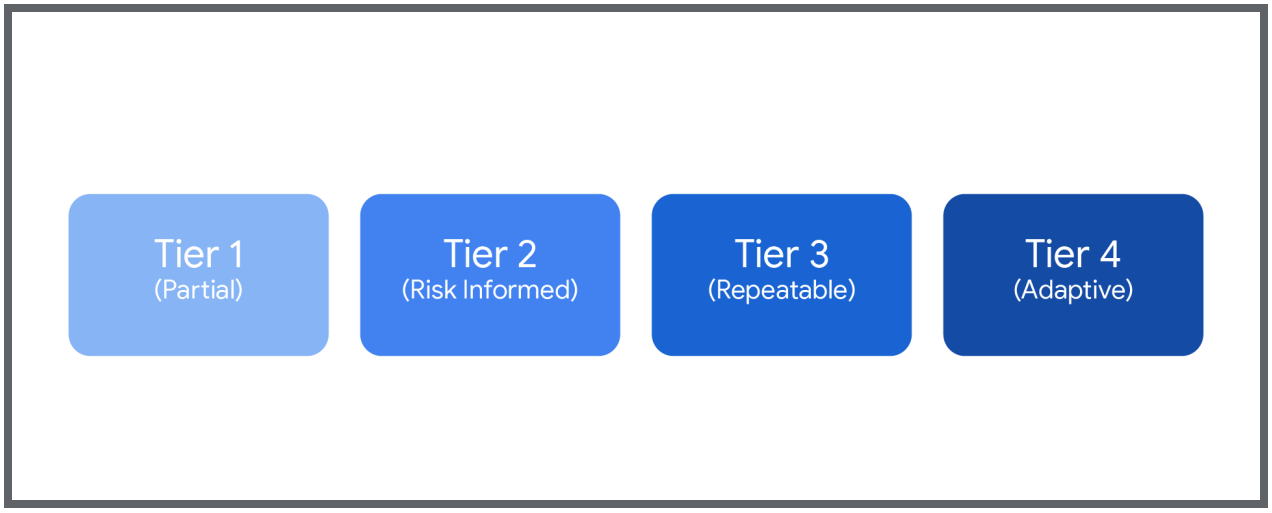
Profiles

Framework Profiles enable organizations to establish a plan for reducing cybersecurity risk that meets organizational goals, considers regulatory requirements and industry standards, and reflects risk management priorities. Organizations may choose to have multiple profiles based on business needs.

Framework Profiles can be used to describe the current state, or the desired target state, of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being met. The Target Profile indicates the desired cybersecurity risk management goals. Comparing Profiles can reveal gaps that need to be addressed to meet cybersecurity risk management objectives.

Implementation Tiers

Tiers describe the degree to which an organization's cybersecurity risk management practices demonstrate the controls defined in the Framework. Each tier increases in thoroughness.
Tier 1 refers to "partial" demonstration of controls
Tier 2 refers to "risk Informed" demonstration of controls
Tier 3 refers to "repeatable" demonstration of controls
Tier 4 is Adaptive



Organizations should determine a desired Tier based on organizational goals, cybersecurity risk levels, and feasibility.

ISO 27001

The ISO 27001 includes 11 sections, called clauses, numbered “0” through “10”, and an “Annex A” that lists specific security controls. Clauses 4 through 10 are considered “mandatory.” An organization must meet the requirements of the mandatory sections to be ISO 27001 compliant.

Clauses 0-3 provide general information about the ISO 27001 standard and include:

- Clause 0: Introduction: Introduces the standard and its purpose.
- Clause 1: Scope: Provides a very high-level view of the information security management system and risk treatment requirements specified within the rest of the standard.
- Clause 2: Normative references: Explains the relationship between ISO 27000 and 27001 standards.
- Clause 3: Terms and definitions: Covers the terminology that is used within the standard.

Clauses 4-10 are mandatory requirements for ISO 27001 certification:

- Clause 4: Context of the organization: Requires documentation that lists external and internal stakeholders, regulatory environments, client lists, competitors, and other industry standards. You must set the boundaries of your system and the controls you will apply.
- Clause 5: Leadership: ISO 27001 compliance requires full support from top management.
- Clause 6: Planning: Based on these risks and opportunities, objectives need to be established, measured and monitored. An organization will need to define and document its criteria for assessing and analyzing risks, and describe how risks will be addressed.
- Clause 7: Support: This clause addresses the resources needed to successfully implement and support an information management system.
- Clause 8: Operation: In the operation clause, an organization will put the plans from clause 6 into action. During this clause the assessments are actually performed and documented.
- Clause 9: Performance evaluation: This clause includes requirements for how to monitor and evaluate the policies, procedures, and controls. It also requires regular internal audits and management reviews.
- Clause 10: Improvement: This clause includes creating a process to log recommendations for improvement that will help an organization eliminate problems,

improve services, and take necessary actions.

Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

The CSA CCM includes 197 control objectives within 17 domains covering key aspects of cloud technology. The controls framework is a common standard for cloud security assurance and compliance.

It consists of a spreadsheet that lists common frameworks and regulations organizations would need to comply with. Each control maps to multiple industry-accepted security standards, regulations, and frameworks. This means that fulfilling the CCM controls also fulfills requirements for many other standards and regulations.

Google Security and Resilience Framework (SRF)

The Google SRF is a foundational risk framework that helps secure adoption of Google Cloud by establishing a set of controls and mapping them to Google security solutions. It provides response and recovery capabilities to ensure the flexibility of workloads running on the Google Cloud platform. The RMF is based on the core functions of NIST: identify, protect, detect, respond, and recover.

Center for Internet Security Controls Framework

The framework includes CIS best practices based on their experience defending organizations against a broad set of cyber threats. The CIS Critical Security Controls are a prescriptive, prioritized, and simplified set of best practices used to strengthen cybersecurity posture. The CIS controls framework helps organizations better identify and assess threats and rapidly adapt to new advanced threats.

Pro tip: Check out the NIST CSF profiles for more industry or subject specific guidance.

Key takeaways

There are many frameworks available for risk management and compliance. As a cloud security professional, it's important for you to know the most common and trusted frameworks. Being familiar with different frameworks and their functions will help you to choose the best controls for the needs of your organization.

Resources for more information

Review these resources to learn more about risk management and security frameworks:

- What is the Cloud Security Control Matrix to learn more about the CSA CCM.
- Google security and resilience framework to explore more about Google security and frameworks.