Google Cloud

Compare and contrast risk management frameworks

You have been learning about frameworks such as SOC 2®, ISO 27001, NIST RMF, and many others. In this reading, you will learn more about the similarities and differences between frameworks and review examples of two combined cloud frameworks that map more than one framework into one document or database. Please note, the following reading should not be considered legal advice.

Key overlaps and differences between SOC 2® and ISO 27001

As you know, frameworks like SOC 2® and ISO 27001 are important for organizations that process or store data. Fortunately, there are overlaps between the two. If you are already working towards SOC 2® compliance, then you are probably meeting some of the obligations of ISO 27001 already.

Two of the key differences between SOC 2® and ISO 27001 are scope and requirements. The goal of ISO 27001 is to provide a framework for how organizations should manage their data and prove they have a working information security management system in place. SOC 2® focuses more narrowly on an organization proving that it has implemented essential data security controls.

Combined frameworks

Similarities and overlaps between frameworks can be used to map controls for multiple frameworks in one document. In this section, you will get an overview and examples of combined frameworks, sometimes called crosswalks, that can be used for audits that cover multiple existing frameworks and compliance obligations.

NIST CSF and SOC 2

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a high-level, risk-based approach to managing cybersecurity, while SOC 2 focuses on proving that a service organization has implemented the necessary security controls.

The American Institute of Certified Public Accountants (AICPA), which oversees SOC 2, has created guidance documents that map its Trust Services Criteria (TSC) to the NIST CSF. This allows organizations to leverage their NIST CSF implementation to demonstrate compliance during a SOC 2 audit, avoiding redundant work.

HITRUST® and SOC 2

HITRUST to SOC 2 mapping is the process of aligning and comparing the security controls and requirements outlined in the HITRUST CSF (Common Security Framework) with those in the SOC 2 framework, specifically the Trust Services Criteria.

While HITRUST and SOC 2 are both widely recognized frameworks, HITRUST covers various industry standards, while SOC 2 focuses more on the management of data based on specific principles like security, availability, and confidentiality.

The goal of mapping is to identify similarities and differences between the two, which can help organizations streamline compliance. By understanding where HITRUST controls satisfy SOC 2 requirements, companies can boost efficiency and limit redundant work.

NIST CSF and SP 800-53

The NIST combined framework maps controls across NIST CSF and SP 800-53.

The SP 800-53 publication provides a comprehensive catalog of specific security and privacy controls. It's a more prescriptive and detailed framework, initially developed as a mandatory standard for U.S. federal agencies and their contractors. The controls are organized into families (e.g., Access Control, Incident Response, Configuration Management) and are the "how-to" for implementing security measures.

NIST's mapping documentation serves as the combined framework. It explicitly links the subcategories of the NIST CSF's five functions to the specific controls in SP 800-53.

Pro tip: Use combined frameworks to perform mega-audits. Mega-audits can audit sets of controls that satisfy several frameworks, such as SOC 2®, ISO 27001, PCI-DSS, and more.

Key takeaways

Knowing the similarities and differences between frameworks can help to streamline the control mapping process. Using combined frameworks enables an organization to check for compliance against multiple frameworks. There are several combined frameworks created by industry leaders that can help you to secure assets and maintain compliance.

Resources for more information

Check out these resources to view the detailed combined framework and control maps.

- SOC 2 and NIST CSF

- HITRUST® and SOC 2
- NIST CSF and SP 800-53