Compare and contrast risk management frameworks

You have been learning about frameworks such as SOC 2®, ISO 31000, 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.

HITRUST®/AICPA® framework

This framework maps controls for both HITRUST® and SOC 2® compliance. HITRUST® and the AICPA® worked together to develop a set of recommendations to streamline and simplify the process of control mapping for both HITRUST® and SOC 2®.

NIST combined framework

The NIST combined framework maps controls across NIST CSF and 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 this resource to learn more:

- HITRUST SOC2 framework to view the detailed combined framework and control map.