Google Cloud

Use existing frameworks to demonstrate compliance

So far, you've learned that compliance is being able to provide evidence that proves that an organization meets certain requirements at a given period in time. You've also learned about the three areas of compliance: people, process and technology. As a cloud security professional, you'll have to ensure that your organization is compliant with a variety of internal and external standards and regulations, depending on the industry that you work in. Frameworks are helpful tools that you can use for compliance and risk management. In this reading, you'll learn how existing frameworks, standards and requirements, like SOC 2®, HITRUST® and the HIPAA Security Rule, can help provide evidence of compliance. Please note, the following reading should not be considered legal advice.

SOC 2® framework

The SOC 2® framework provides a set of auditing standards and guidelines to ensure that the organization's information security practices and procedures align with the American Institute of Certified Public Accountants' (AICPA) Trust Services Criteria. Licensed Certified Personal Accountants (CPAs) use the auditing standards to issue a SOC 2® report. Presenting users with this report gives them confidence that the controls presented in the SOC 2® report are effective. Effectiveness of controls is measured against the Trust Services Criteria. The Trust Services Criteria are also used by service organization management to assess the effectiveness of controls in preparation for a CPA's SOC 2® audit. Evidence of each necessary control is required to demonstrate that an organization meets the SOC 2® standards.

SOC 2® focuses on five Trust Service Categories (TSCs):

1. Security
2. Availability
3. Processing Integrity
4. Confidentiality
5. Privacy

One of the most important decisions when pursuing a SOC 2® report is to decide which TSCs to include in the scope of your audit. While a SOC 2® report can cover any (or all) of the five areas, many just cover two or three of the five.

NIST Cybersecurity Framework (CSF)

As you've learned, The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), is a voluntary framework that captures standards, guidelines, and best practices to manage cybersecurity-related risk. The framework maps to many existing information security frameworks. The CSF is both detailed and accessible, and it's used by many organizations around the world. Though the CSF was originally written for the protection of critical infrastructure in the United States (US), the framework is now used in other US industries, including transportation, banking, and healthcare.

NIST generalizes cybersecurity activities into five core functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

These functions help guide organizations with mapping out the management of cybersecurity risks. Organizations should perform these functions concurrently, continuously, and regularly to establish an operational culture for dynamically addressing cybersecurity risks.

The NIST CSF includes both standards and specific controls that organizations can adopt to meet compliance obligations. There is no formal certification or accreditation program for NIST CSF.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) set standards in the US to protect individually identifiable health information. HIPAA applies to health plans, most healthcare providers, and healthcare clearinghouses—collectively known as *covered entities*—that manage protected health information (PHI) and to persons or entities that perform certain functions on their behalf, known as *business associates*.

The HIPAA Privacy Rule requires covered entities and their business associates to safeguard the privacy of PHI handled in any medium, while the HIPAA Security Rule obligates them to protect the confidentiality, integrity, and availability of PHI they create, receive, maintain, or transmit electronically with administrative, physical, and technical measures. Covered entities and business associates also have breach notification obligations and duties.

HITRUST®

The HITRUST Cybersecurity Framework (CSF)®, is a set of prescriptive controls organizations can use to meet healthcare information security regulations. HITRUST® includes these security categories:

- Information Security Management Program
- Access Control
- Human Resources Security
- Risk Management
- Security Policy
- Organization of Information Security
- Compliance
- Asset Management
- Physical and Environmental Security
- Communications and Operations Management
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Privacy Practices

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard that provides a baseline of technical and operational requirements designed to protect account data. PCI DSS includes security practices, technologies, processes, and standards for merchants, service providers, and financial institutions.

The PCI DSS v4 standard requires that organizations maintain a secure network, system, and vulnerability management program. The standard also requires organizations to protect account data, implement strong access control measures and information security policies, and monitor and test networks regularly.

Key takeaways

Industry standard frameworks that can be useful tools on your journey to compliance include SOC 2®, HITRUST®, the HIPAA Security Rule and PCI DSS. Using established controls and questions that are proven effective will help you to meet compliance obligations based on your organization's needs.

Resources for more information

Check out these resources for more information about frameworks:

- HIPAA Security Series to learn more about the HIPAA Security Rule
- Use HITRUST® for HIPAA compliance to learn more about using HITRUST® framework to comply with HIPAA.
- Example of the NIST Cybersecurity Framework and Google Cloud