RESOURCE CENTER

Achieve SOC 2 password compliance with Bitwarden

Get the full interactive view at https://bitwarden.com/resources/achieve-soc-2-password-compliance-with-bitwarden/

bitwarden

Companies that provide services to other organizations and are seeking to boost their information security stance often complete a Service Organization Control 2 (SOC 2) audit, with a growing focus on meeting SOC 2 password requirements. The SOC 2 certification process includes demonstrating adequate system access controls to ensure that sensitive data remains protected and secured at all times. SOC 2 reports are often requested by customers and business partners of outsourced solution providers, underscoring the importance of SOC 2 compliance. Many companies seeking SOC 2 compliance leverage solutions such as a SOC 2-compliant password manager to help meet requirements.

> Check out the Resource Center for more guides on how to achieve compliance with other security standards.

Table of Contents

A summary of SOC 2 trust services criteria

SOC 2 reports are relevant to service organizations and pertain to the controls concerning aspects like security and privacy. The American Institute of Certified Public Accountants (AICPA) introduced the Service Organization Control or SOC 2 report to help evaluate service companies – i.e., financial firms, healthcare providers, cloud service providers, and SaaS providers – and their ability to maintain strong controls "relevant to security, availability, and processing integrity of the systems … to process users' data and the confidentiality and privacy of the information processed by these systems."

SOC 2 includes two types of reports:

- Type 1: Reports on a company's system description and the suitability of the design of its controls.
- Type 2: Reports on a company's system description and the suitability *and* operational effectiveness of its controls.

During SOC 2 audits, a service organization's controls are evaluated to ensure compliance with the security framework. Both SOC 2 report types detail how companies process data, but SOC 2 Type 2 more deeply describes data security controls in place, including credential management. Both report types are restricted to certain entities (e.g., customers or auditors). However, companies may also produce a publicly available SOC 3 report, which summarizes some of the data security criteria found in the SOC 2 report.

> Check out the Bitwarden SOC 3 Report.

Overview of the SOC 2 certification process

Companies seeking SOC 2 certification must pass an audit conducted by an accredited AICPA representative. The five Trust Services Criteria form the fundamental components of the SOC 2 compliance framework, including Security, Availability, Processing Integrity, Confidentiality, and Privacy. First developed in 2017, and last updated in late 2022 to "reflect an environment of ever-changing technologies, threats, and vulnerabilities … changing legal and regulatory requirements and related cultural expectations regarding privacy," and "addressing data management, particularly when related to confidentiality," the criteria is as follows:

- **Security** - Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, data integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.
- **Availability** - Information and systems are available for operation and used to meet the entity's objectives.
- **Processing integrity** - System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality** - Information designated as confidential is protected to meet the entity's objectives.
- **Privacy** - Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Internal controls play a crucial role in ensuring compliance with the Trust Services Criteria during audits.

Companies only have to comply with the principles that apply to them. For example, the Availability Principle typically applies to companies providing customers with colocation, data center, SaaS-based services, or hosting services.

You might also like:

The benefits of password managers for finance companies

The Security Principle: SOC 2 security controls and password requirements

The Security Principle applies to most companies seeking SOC 2 compliance, focusing on protecting customer data. The bulk of the Security Principle requirements exist under section CC6 of the Trust Services Criteria, which also details SOC 2 password requirements. The following sections demonstrate how a password manager can support many key requirements.

SOC 2 controls are significant in mitigating data breaches and protecting sensitive information.

Infrastructure credentials management to protect customer data

> "The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives." - CC6.1 (Pg. 34-35)

Companies must demonstrate how they manage credentials for infrastructure and software, including removing access once it's no longer needed or required. With a password manager, administrators can easily automate access, assign roles, and restrict users to read-only access for system credentials. Granular access control allows administrators to hide credentials to prevent copying passwords, TOTP seeds, or custom fields.

An accredited CPA evaluates an organization's controls' design and operating effectiveness during a SOC 2 audit to ensure they align with the required standards for safeguarding sensitive data.

Companies must encrypt their data and protect encryption keys at all times. With a 100% end-to-end zero-knowledge encrypted password manager using AES 256-bit encryption, companies protect their credentials and sensitive information that can be shared amongst employees, such as financial documents. Additionally, PBKDF2 SHA-256 strengthens encryption key protection by limiting key retrieval to only the user logging in with their master password.

Onboarding and succession

> "Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized." - CC6.2 (Pg. 36)

Companies must show how they register and authenticate new users, including levels of access. With a password manager, administrators can link their directory service (LDAP) to streamline user onboarding and succession. Users and groups in your company LDAP sync with your password manager's Organization, replicating the same structure. Better yet, whenever a new user is added to the LDAP, they are also created in the password manager—and vice versa, they are removed when de-provisioned from the LDAP.

Companies must authorize access to protected assets. A password manager with Single Sign On allows your existing Identity Provider to offer authentication for password manager users. Administrators can set password policies requiring users to log in through the Single Sign-On method to access credentials.

Granular access control

> "The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives." - CC6.3 (pg. 36)

Companies must demonstrate role-based access controls (RBAC). With a password manager, administrators can set user types and create custom roles to assign granular control and user permissions for components of the password manager. Role-based access controls can be configured for functions such as who can manage users, access event logs, or import/export data.

Wondering how else to boost your company's security? Check out Bitwarden Secrets Manager to secure your developer secrets.

Explore Bitwarden to support SOC 2 compliance and password requirements

Adding a password manager, such as Bitwarden, can demonstrate the commitment of service providers to protect customer data and SOC 2 auditors. Bitwarden offers enterprise-grade security, conducts regular third-party security audits, and complies with major privacy and security standards, including SOC 2.

Bitwarden supports service organizations in meeting SOC 2 compliance requirements by ensuring effective controls are in place for safeguarding data.

Take advantage of an all-access free Enterprise trial to see how Bitwarden can help service providers prepare for a SOC 2 security audit and meet SOC 2 password requirements.

Read more:

How to choose the best enterprise password manager for your business