SECURISEA

SOC 2 Assessment Checklist

Introduction

Here's a comprehensive SOC 2 Assessment Checklist designed for organizations seeking SOC 2 compliance for the first time. This checklist will help you prepare for a SOC 2 audit by focusing on the essential criteria across the five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy). The checklist ensures that your systems, policies, and controls align with the SOC 2 framework.

1. Define Your Scope

- Identify Trust Service Principles (TSPs) to Include: Choose which of the five TSPs are relevant to your business:
    - Security (required)
    - Availability
    - Processing Integrity
    - Confidentiality
    - Privacy
- Identify Systems & Services: Document the systems, applications, and services that fall within the SOC 2 scope.
- Define Boundaries: Identify any third-party vendors or cloud services and determine how they are involved, if these vendors are essential for any aspects of your SOC2 compliance, they should be listed as 'subservice organizations'
- Consider if any of your controls require specific user actions to be effective, in this case each of those items should be listed a 'complementary user entity controls' or CUECs

2. Establish Security Policies and Procedures

- **Develop a Security Policy:** Document a formal security policy outlining security objectives, guidelines, and roles.
- **Access Control Policy:** Establish user access levels, least privilege, and segregation of duties.
- **Incident Response Plan:** Create a plan to address security incidents, including roles, communication strategies, and response procedures.

- **Risk Management Policy:** Define risk assessment processes, including how to identify and mitigate risks.
- **Change Management Policy:** Document the procedures for managing and tracking changes to your systems.

3. Implement and Document Security Controls

- **User Authentication:** Implement multi-factor authentication (MFA) for users accessing sensitive systems.
- **Access Reviews:** Regularly conduct user access reviews to ensure only authorized users have access to systems.
- **Encryption:** Ensure that sensitive data is encrypted both in transit and at rest.
- **Firewall and Network Security:** Deploy firewalls and intrusion detection/prevention systems to secure the network.
- **Logging and Monitoring:** Implement log management for security events and ensure logs are regularly reviewed for anomalies.
- **Patch Management:** Develop a schedule for updating and patching software and systems.
- **Data Backup and Recovery:** Ensure regular backups of critical systems, with documented recovery procedures.

4. Vendor Management and Third-Party Risk

- **Vendor Due Diligence:** Conduct security evaluations for all third-party vendors involved in processing your data.
- **Third-Party Contracts:** Ensure contracts with third-party vendors include clauses related to SOC 2 compliance and data protection.

5. Employee Training and Awareness

- **Security Awareness Training:** Conduct regular security training for all employees to ensure they are aware of best practices.
- **Confidentiality Agreements:** Ensure all employees sign confidentiality agreements as part of their employment.

6. System Availability and Monitoring

- **Uptime Monitoring:** Implement tools to monitor system uptime and availability.
- **Disaster Recovery Plan:** Create a formal disaster recovery plan, including failover procedures and communication strategies.

- **Capacity Planning:** Document how your organization monitors and maintains sufficient capacity to meet operational demands.

7. Data Integrity and Confidentiality Controls

- **Data Classification:** Classify sensitive data (e.g., PII, financial information) and document procedures for handling it.
- **Data Retention Policy:** Define a policy for data retention and disposal, ensuring secure deletion of obsolete data.
- **Data Access Auditing:** Implement procedures to track and log access to confidential data.

8. Privacy Controls (If Applicable)

- **Privacy Policy:** Develop a formal privacy policy aligned with SOC 2 privacy requirements.
- **Consent Management:** Ensure processes are in place for collecting and managing user consent for data processing.
- **Right to Access:** Implement procedures for allowing individuals to access, correct, or delete their personal data.

9. Perform a Risk Assessment

- **Risk Identification:** Identify all risks related to your information security program.
- **Risk Mitigation:** Develop action plans to address and mitigate risks.
- **Document Risk Assessments:** Ensure all risk assessments are formally documented.

11. Prepare for the External Audit

- **Select an Independent Auditor:** Choose a certified SOC 2 auditor to conduct the audit.
- **Documentation Readiness:** Ensure all policies, procedures, and security controls are documented and accessible to the auditor.
- **Conduct a Readiness Assessment:** Perform a final readiness assessment to ensure your organization is fully prepared for the audit.
-

This checklist serves as a guide for organizations approaching SOC 2 compliance for the first time. It helps ensure your systems and processes meet the necessary requirements for a successful SOC 2 audit, building trust with your customers and stakeholders.

SECURISEA

Simplifying security compliance since 2006

LEARN MORE