NDB

SOC 2

Readiness Checklist for Organizations

Audit Readiness

This checklist is designed to guide your organization through the process of preparing for a SOC 2 audit. By following these action items, you can ensure that all necessary steps are taken to meet compliance requirements and pass the audit smoothly.

NDB

SOC 2 Readiness Checklist

1 Determine If a GRC Tool is to Be Used

Evaluate Governance, Risk, and Compliance (GRC) Tools

	COMPLETE ? YES	NO
☐ Consider using a GRC tool like Vanta, Drata, or Secureframe to streamline your SOC 2 compliance process.	☐	☐
☐ Ensure the selected GRC tool aligns with your organization's needs, such as audit management, policy generation, and task tracking.	☐	☐

Assign Internal Personnel

☐ Identify personnel responsible for administering and working within the GRC tool (e.g., IT, compliance, or legal departments).	☐	☐

Assign Ownership

☐ Designate specific team members to manage GRC tool operations, including user management, policy updates, and tracking compliance progress.	☐	☐

Train Internal Users

☐ Ensure proper training for internal users working with the GRC tool to ensure familiarity with the system and its capabilities.	☐	☐

2 Secure Senior Leadership Buy-In

Action Items:

- ☐ Ensure that senior leadership understands the importance of SOC 2 compliance and its impact on the organization's reputation and risk management.
- ☐ Communicate the benefits of SOC 2 compliance (e.g., enhanced customer trust, competitive advantage, and risk mitigation).
- ☐ Allocate necessary resources (budget, time, personnel) to support the compliance initiative.
- ☐ Appoint a senior leader or team to oversee SOC 2 readiness.
- ☐ Promote SOC 2 compliance as a company-wide priority to ensure alignment across departments.

COMPLETE ?

☐ YES ☐ NO

3 Make a Cultural Shift Toward Embracing Compliance

Action Items:

- ☐ Foster a culture of security and compliance by including all employees in the process.
- ☐ Provide company-wide training on SOC 2 compliance and the importance of cybersecurity hygiene.
- ☐ Lead by example – senior management should adhere to the same compliance policies as all employees.
- ☐ Regularly communicate the importance of SOC 2 and its relevance to the company's success.
- ☐ Recognize and reward teams that demonstrate good security practices and compliance.

COMPLETE ?

☐ YES ☐ NO

4 Properly Scope the Audit (Business Processes, Technologies, People)

Action Items:

- ☐ Identify all business processes that handle sensitive customer data (e.g., customer onboarding, payment processing).
- ☐ List all technologies that process, store, or transmit sensitive data (cloud platforms, software, servers, etc.).
- ☐ Identify key personnel responsible for implementing security controls and maintaining compliance.
- ☐ Document any third-party vendors with access to sensitive data or systems and ensure they are included in the audit scope.
- ☐ Develop a clear map of data flow to ensure all touchpoints are captured in the scope.

COMPLETE ?

☐ **YES** ☐ **NO**

5 Establish a Company-Wide System of Internal Controls for Cyber Hygiene

Action Items:

- ☐ Implement and document internal controls for access management, password policies, and system security.
- ☐ Define and implement endpoint security protocols (antivirus, firewalls, device encryption).
- ☐ Ensure regular patching and software updates for all systems.
- ☐ Set up access control mechanisms such as role-based access control (RBAC) and multi-factor authentication (MFA).
- ☐ Monitor and review internal controls regularly for compliance and improvements.

COMPLETE ?

☐ **YES** ☐ **NO**

6 Develop Information Security Policies and Procedures

Action Items:

Draft or update the following policies and procedures to meet SOC 2 requirements

COMPLETE ?

YES NO

- ☐ **Access Control Policy:** Define access permissions, roles, and authentication methods.
- ☐ **Data Classification and Handling Policy:** Outline how sensitive data should be classified, handled, stored, and disposed of.
- ☐ **Change Management Policy:** Create a process for managing and documenting system and software changes.
- ☐ **Risk Management and Assessment Procedure:** Formalize how risks will be identified, assessed, and mitigated.
- ☐ **Employee Onboarding and Offboarding Procedures:** Ensure secure access to systems during onboarding and remove access during offboarding.
- ☐ **Vendor Management Policy:** Define how third-party vendors will be assessed and managed for security compliance.
- ☐ **Encryption and Key Management Policy:** Establish rules for data encryption, key storage, and key management.
- ☐ **System and Network Security Policy:** Document how systems and networks will be secured (firewalls, intrusion detection, etc.).
- ☐ **Logging and Monitoring Policy:** Set up systems for monitoring and logging critical activities across systems.
- ☐ **Physical Security Policy:** Protect physical access to sensitive systems and data.
- ☐ **Privacy Policy:** Ensure compliance with data privacy regulations (GDPR, CCPA, etc.).

6 [Continued] Develop Information Security Policies and Procedures

Action Items:

Draft or update the following policies and procedures to meet SOC 2 requirements

COMPLETE ?

YES NO

- ☐ **Audit and Compliance Monitoring Procedures:** Define how audits will be conducted and how compliance will be monitored.
- ☐ **Acceptable Use Policy:** Define acceptable and unacceptable uses of company systems and data.
- ☐ **Data Retention and Disposal Policy:** Outline how long data will be kept and secure methods for data disposal.
- ☐ **Third-Party Risk Management Policy:** Implement a process for assessing the security risks of third-party vendors.
- ☐ **Security Awareness Training Policy:** Develop a policy for continuous security training for employees.
- ☐ **Multi-Factor Authentication (MFA) Policy:** Enforce MFA for accessing critical systems and data.
- ☐ **Backup and Recovery Policy:** Establish regular backup procedures and a recovery plan for critical systems.
- ☐ **Software Development and Secure Coding Standards:** Ensure secure coding practices are followed in software development.
- ☐ **Patch Management Policy:** Define how software patches will be applied across the organization.
- ☐ **Monitoring and Alerting Policy:** Set up a system for monitoring and alerting on suspicious activities and vulnerabilities.
- ☐ **Service-Level Agreement (SLA) Management:** Define service expectations and response times with third-party providers.

7 Develop and Implement a Formal Enterprise-Wide Risk Assessment Program

Action Items:

- ☐ Conduct a comprehensive risk assessment to identify and evaluate threats to information security, availability, confidentiality, and privacy.
- ☐ Prioritize risks based on their potential impact on the organization and the likelihood of occurrence.
- ☐ Develop a risk mitigation plan for each identified risk.
- ☐ Implement controls and continuously monitor risk levels.
- ☐ Document the risk assessment process and keep records for future audits.

COMPLETE ?

☐ YES ☐ NO

8 Have a Master Asset Inventory in Place

Action Items:

- ☐ Create and maintain an up-to-date asset inventory that includes hardware, software, and third-party services.
- ☐ Include details such as asset ownership, location, security status, and lifecycle.
- ☐ Review the inventory regularly to ensure accuracy.
- ☐ Ensure the asset inventory is integrated with other systems like change management and vendor management.

COMPLETE ?

☐ YES ☐ NO

9 Develop and Implement a Formal Enterprise-Wide Risk Assessment Program

Action Items:

- ☐ Set up continuous monitoring for all systems handling sensitive data.
- ☐ Configure automated alerting for anomalous activities such as unauthorized access attempts or system failures.
- ☐ Implement logging to capture critical system events, access logs, and error messages.
- ☐ Create a reporting system that tracks security events and system performance metrics.

COMPLETE ?

☐ YES ☐ NO

10 Establish a Formal Incident Response Program

Action Items:

- ☐ Develop a detailed Incident Response Plan (IRP) that outlines procedures for identifying, containing, and remediating security incidents.
- ☐ Define roles and responsibilities for incident response teams.
- ☐ Establish communication protocols for notifying stakeholders, customers, and regulatory bodies.
- ☐ Regularly conduct incident response drills to ensure teams are prepared to act swiftly.

COMPLETE ?

☐ YES ☐ NO

11 Establish a Formal Business Continuity Plan

Action Items:

- ☐ Identify essential business processes that must continue in the event of a disaster.
- ☐ Develop recovery strategies for critical systems and data.
- ☐ Test the business continuity plan through simulations and real-world exercises.
- ☐ Review and update the business continuity plan annually to account for new risks and technologies.

COMPLETE ?

☐ **YES** ☐ **NO**

12 Implement a Formal Third-Party Vendor Management Program

Action Items:

- ☐ Develop a detailed Incident Response Plan (IRP) that outlines procedures for identifying, containing, and remediating security incidents.
- ☐ Include security requirements in contracts with vendors and service providers.
- ☐ Regularly monitor vendor performance to ensure compliance with agreed-upon standards.
- ☐ Create an ongoing process for assessing and re-assessing vendor risk.

COMPLETE ?

☐ **YES** ☐ **NO**

13 Implement a Formal Continuous Monitoring Program

Action Items:

- ☐ Set up continuous monitoring of systems, network traffic, user behavior, and key performance indicators.
- ☐ Implement a system to identify vulnerabilities, security incidents, and potential threats in real time.
- ☐ Regularly review monitoring processes and ensure they are aligned with evolving compliance requirements.
- ☐ Document monitoring processes and maintain records of incidents and actions taken.

COMPLETE ?

☐ YES ☐ NO

13 Final Steps: Ongoing Review and Preparation

Action Items:

- ☐ Conduct regular internal audits to ensure that controls are working effectively and remain compliant with SOC 2 standards.
- ☐ Schedule external audits to verify compliance and identify areas for improvement.
- ☐ Ensure that senior leadership is regularly updated on progress and challenges related to SOC 2 readiness.
- ☐ Prepare for a SOC 2 Type 1 audit (point-in-time audit) and then progress to a SOC 2 Type 2 audit (over a defined period) once readiness has been achieved.

COMPLETE ?

☐ YES ☐ NO

SOC Audit Readiness

Talk With An Audit Expert Today

SOC 2 Audit Experts

Preparing for a SOC 2 audit can be a complex and detailed process, but with the right planning, resources, and dedication, your organization can achieve the necessary compliance to safeguard sensitive data and build trust with customers.

From selecting a GRC tool to implementing internal controls, policies, and risk management programs, each step is crucial for a successful SOC 2 audit. If your organization needs expert guidance or assistance in navigating the SOC 2 readiness journey, NDB is here to help.

Our team of professionals specializes in guiding companies through the SOC 2 process, ensuring you're fully prepared for both Type 1 and Type 2 audits. Reach out to NDB today and learn how we can support your compliance efforts and help you achieve a seamless SOC 2 certification.

NDB CPA

ndbcpa.com
214-272-0967

NDB