Vanta

Compliance Requirements for SOC 2 Checklist

Compliance Requirements for SOC 2 Checklist

SOC 2 attestation is one of the best assets your business can have, especially when it comes to opening doors to a more diverse pool of clients and partners.

Achieving and maintaining your SOC 2 compliance can be time-consuming and expensive, but it's less so if you start with a thorough understanding of SOC 2 reports and the SOC 2 compliance requirements.

An overview of SOC 2 compliance requirements

For starters, let's look at how the SOC 2 compliance requirements are organized. Within SOC 2, there are five categories known as the five **Trust Services Criteria:** security, availability, processing integrity, confidentiality, and privacy.

There are 17 principles that apply to all five of these Trust Services Criteria. Within those principles, there are also more specific areas of focus that apply to only certain trust services criteria.

The good news is that only the security criteria are truly mandatory for all organizations seeking SOC 2 compliance. The other four criteria are only required on an "as applicable" basis depending on your organization and your framework.

This checklist is the list of SOC 2 guidelines that are required for any organization seeking compliance.

COSO framework

The Committee of Sponsoring Organizations (COSO) framework is a system used to establish internal controls within an organization to assess risk management. The 17 principles of the COSO framework are the key requirements for SOC 2 compliance.

CONTROL COMPONENT 1

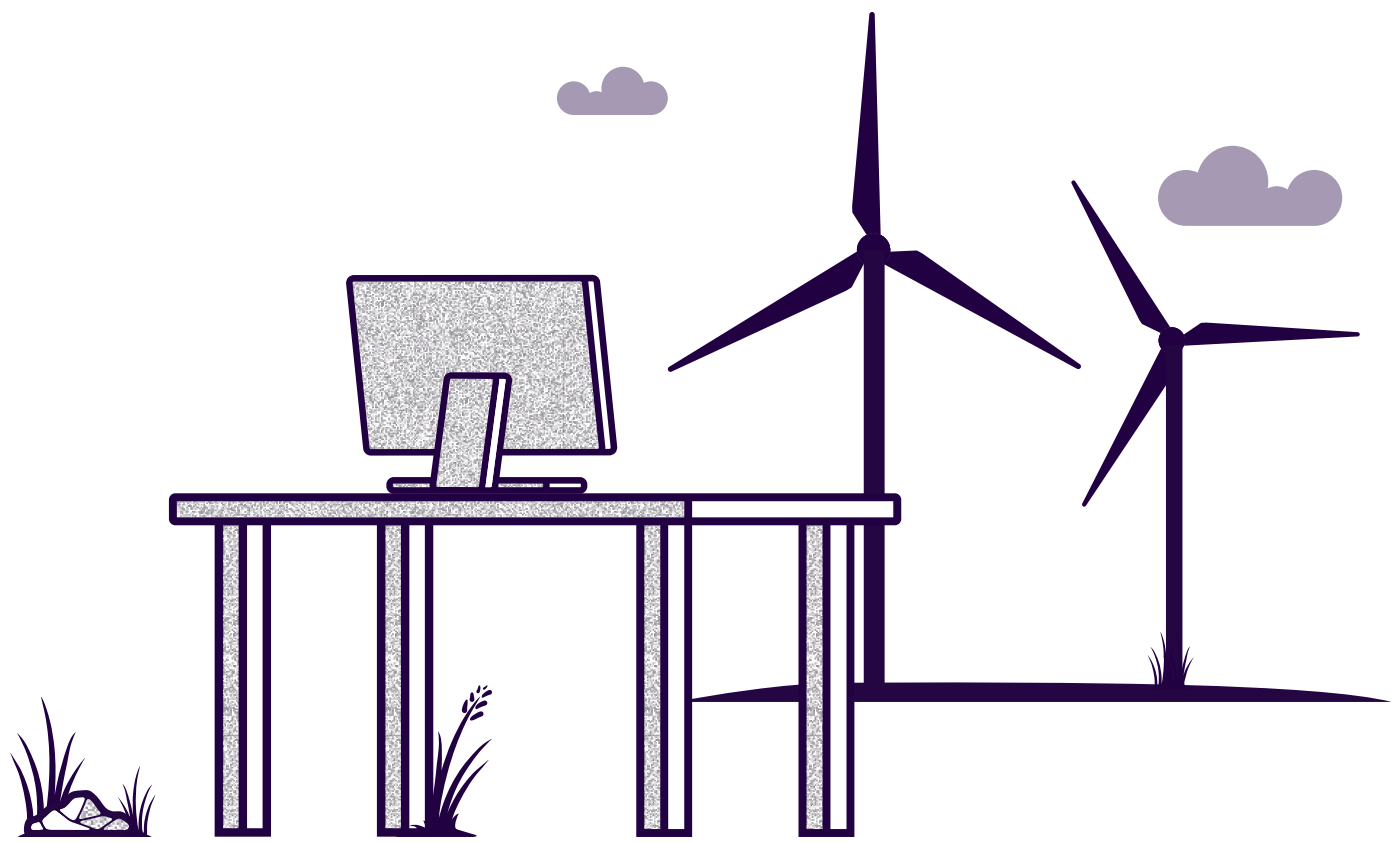
Control environment:

- [ ] **CC1.1: Demonstrate a commitment to integrity and ethical values:**
  - → Set the tone at the top with integrity among top-tier management
  - → Establish standards of conduct
  - → Regularly evaluate adherence to the standards of conduct
  - → Address deviations from the standards of conduct in a timely manner
- [ ] **CC1.2: Your board of directors operates independently of management and oversees the development and performance of internal control:**
  - → Establish oversight responsibilities
  - → Apply relevant expertise among the board of directors
  - → Operate independently from management
- [ ] **CC1.3: Management establishes structures, reporting lines, and authorities or responsibilities with board oversight**
  - → Consider all structures of the organization
  - → Establish reporting lines
  - → Define, assign, and limit authorities and responsibilities
- [ ] **CC1.4: Demonstrate a commitment to attract, develop, and retain competent employees in alignment with objectives:**
  - → Establish policies and practices
  - → Evaluate competence and address shortcomings
  - → Attract, develop, and retain competent individuals
  - → Plan and prepare for succession
- [ ] **CC1.5: Hold individuals responsible for their internal control responsibilities:**
  - → Enforce accountability through established structures, authorities, and responsibilities
  - → Establish performance measures, incentives, and rewards
  - → Evaluate performance measures, incentives, and rewards for relevance on an ongoing basis
  - → Consider excessive pressures
  - → Evaluate performance routinely and reward or discipline employees

CONTROL COMPONENT 2

Communication and information:

- [ ] **CC2.1: Obtain or generate and use relevant, quality information to support the functioning of internal control:**
  - → Identify information requirements
  - → Capture internal and external sources of data
  - → Process relevant data for information
  - → Maintain quality throughout processing
- [ ] **CC2.2: Internally communicate information, including objectives and responsibilities for internal control, necessary to support internal control:**
  - → Communicate internal control information
  - → Communicate with the board of directors
  - → Provide separate communication lines
  - → Select a relevant method of communication
- [ ] **CC2.3: Communicate with external parties on matters that affect internal control:**
  - → Communicate to external parties
  - → Enable inbound communication
  - → Communicate with the board of directors
  - → Provide separate communication lines
  - → Select a relevant method of communication



CONTROL COMPONENT 3

Risk assessment:

- [ ] **CC3.1: Specify objectives with adequate clarity to allow for the identification and assessment of risks relating to objectives:**
  - **Points of focus for operations objectives:**
    - → Reflect management's choices
    - → Consider tolerance for risk
    - → Include operations and financial performance goals
    - → Form a basis for committing resources
  - **Points of focus for external financial reporting objectives:**
    - → Comply with applicable accounting standards
    - → Take materiality into consideration
    - → Reflect entity activities
  - **Points of focus for external non-financial reporting objectives:**
    - → Comply with externally established frameworks as applicable
    - → Consider the required level of precision
    - → Reflect entity activities
  - **Points of focus for internal reporting objectives:**
    - → Reflect management's choices
    - → Consider the required level of precision
    - → Reflect entity activities
  - **Points of focus for compliance objectives:**
    - → Reflect external laws and regulations
    - → Consider tolerance for risk
- [ ] **CC3.2: Identify risks to the achievement of your objectives across the organization and analyze risks to determine how the risks should be managed:**
  - → Include entity, subsidiary, division, operating unit, and functional levels
  - → Analyze internal and external factors
  - → Involve appropriate levels of management
  - → Estimate the significance of the risks identified
  - → Determine how to respond to risks
- [ ] **CC3.3: Consider the potential for fraud in assessing risks to achieving the objectives:**
  - → Consider various types of fraud
  - → Assess incentives and pressures
  - → Assess opportunities for fraud
  - → Assess attitudes and rationalizations

- [ ] **CC3.4: Identify and assess changes that could significantly impact the system of internal control:**
  - → Assess changes in the external environment
  - → Assess changes in the business model
  - → Assess changes in leadership

CONTROL COMPONENT 4

Monitoring activities:

- [ ] **CC4.1: Select, develop, and perform ongoing and/or separate evaluations to determine whether the components of internal control are present and functioning:**
  - → Consider a combination of ongoing and separate evaluations
  - → Consider the rate of change
  - → Establish a baseline understanding
  - → Use knowledgeable personnel
  - → Integrate with business processes
  - → Adjust the scope and frequency as needed
  - → Evaluate objectively
- [ ] **CC4.2: Evaluate and communicate internal control deficiencies promptly to those responsible for taking corrective action:**
  - → Assess evaluation results
  - → Communicate deficiencies
  - → Monitor corrective actions

CONTROL COMPONENT 5

Control activities:

- [ ] **CC5.1: Select and develop control activities that help to mitigate risks to the acceptable achievement of objectives:**
  - → Integrate with risk assessment
  - → Consider entity-specific factors
  - → Determine relevant business processes
  - → Evaluate a mix of control activity types
  - → Consider at what level activities are applied
  - → Address segregation of duties

- [ ] **CC5.2: Select and develop general control activities over technology to support the achievement of objectives:**
  - → Determine dependency between the use of technology in business processes and technology general controls
  - → Establish relevant technology infrastructure control activities
  - → Establish relevant security management process control activities
  - → Establish relevant activity controls for technology acquisition, development, and maintenance processes
- [ ] **CC5.3: Deploy control activities through policies that establish what is expected and in policies that put procedures into action:**
  - → Establish policies and procedures to support deployment of management's directives
  - → Establish responsibility and accountability for executing procedures and policies
  - → Perform in a timely manner
  - → Take corrective action
  - → Perform using competent personnel
  - → Reassess policies and procedures

CONTROL COMPONENT 6

Logical and physical access controls:

- [ ] **CC6.1: Implement logical access security software, infrastructure, and architecture over protected information assets to protect them from security events to meet the organization's objectives:**
  - → Identify and manage the inventory of information assets
  - → Restrict logical access
  - → Identify and authenticate users
  - → Consider network segmentation
  - → Identify points of access
  - → Restrict access to information assets
  - → Manage identification and authentication
  - → Manage credentials for infrastructure and software
  - → Use encryption to protect data
  - → Protect encryption keys
- [ ] **CC6.2: Register and authorize all internal and external users whose access is granted by your organization before issuing credentials and providing access, and promptly remove access from those who are no longer authorized:**
  - → Control credentials for access to protected assets
  - → Remove access to protected assets when appropriate
  - → Review appropriateness of access controls

- [ ] **CC6.3: Authorize, modify, and remove access to all protected information (data, software, functions, etc) based on roles, responsibilities, and system design and changes with a focus on granting the least privilege and on segregation of duties:**
  - → Create or modify access to protected information assets as warranted
  - → Remove access to protected information assets as warranted
  - → Use role-based access controls
  - → Review access roles and rules
- [ ] **CC6.4: Restrict physical access to facilities and protected information assets to authorized personnel:**
  - → Create or modify physical access as warranted
  - → Remove physical access as warranted
  - → Review physical access routinely
- [ ] **CC6.5: Discontinue logical and physical protections over physical assets only after the ability to read or recover any data or software from those assets has been diminished:**
  - → Identify data and software for disposal
  - → Remove data and software from the organization's control
- [ ] **CC6.6: Implement logical access security measures to protect against external threats:**
  - → Restrict access
  - → Protect identification and authentication credentials
  - → Require additional authentication or credentials for anyone accessing assets from outside the system
  - → Implement boundary protection systems
- [ ] **CC6.7: Restrict the transmission, movement, and removal of information to authorized users and processes, and protect it during any transmission, movement, or removal:**
  - → Restrict the ability to transmit data
  - → Use encryption technologies or secure communication channels to protect data
  - → Protect removal media
  - → Protect mobile devices
- [ ] **CC6.8: Implement controls to prevent or detect and act upon any malicious software:**
  - → Restrict application and software installation
  - → Detect unauthorized changes to software and configuration parameters
  - → Use a defined change control process
  - → Use antivirus and anti-malware software
  - → Scan information assets from outside the organization for malware and other unauthorized software

CONTROL COMPONENT 7

System operations:

- [ ] **CC7.1: Use detection and monitoring procedures to identify configuration changes that result in the introduction of new vulnerabilities and identify susceptibilities to newly discovered vulnerabilities:**
  - → Use defined configuration standards
  - → Monitor infrastructure and software
  - → Implement change detection mechanisms
  - → Detect unknown or unauthorized components
  - → Conduct vulnerability scans routinely
- [ ] **CC7.2: Monitor system components and the operation of those components for anomalies that may indicate malicious acts, natural disasters, and errors, and analyze these anomalies to determine whether they represent security events:**
  - → Implement detection policies, procedures, and tools
  - → Design anomaly detection measures
  - → Implement filters to analyze anomalies
  - → Monitor detection tools for effective operation
- [ ] **CC7.3: Evaluate security events to determine whether they could or have resulted in a failure of the organization/entity to meet your objectives (security incidents), and if so, take action to prevent or address these failures:**
  - → Respond to security incidents
  - → Communicate and review detected security events
  - → Develop and implement procedures to analyze security incidents
- [ ] **CC7.4: Respond to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents:**
  - → Assign roles and responsibilities
  - → Contain security incidents
  - → Mitigate ongoing security incidents
  - → End threats posed by security incidents
  - → Restore operations
  - → Develop and implement communication protocols for security incidents
  - → Obtain an understanding of the nature of each incident and determine a containment strategy
  - → Remediate identified vulnerabilities
  - → Communicate remediation activities
  - → Evaluate the effectiveness of incident responses
  - → Periodically evaluate incidents

- [ ] **CC7.5: Identify, develop, and implement activities to recover from identified security incidents:**
  - → Restore the affected environment
  - → Communicate information about the event
  - → Determine the root cause of the event
  - → Implement changes to prevent and detect recurrences
  - → Improve response and recovery procedures
  - → Implement incident recovery plan testing

CONTROL COMPONENT 8

Change management:

- [ ] **CC8.1: Authorize, design, develop or acquire, configure, document, test, approve, and implement changes to infrastructure, data, software, and procedures:**
  - → Manage changes throughout the system lifecycle
  - → Authorize changes
  - → Design and develop changes
  - → Document changes
  - → Track system changes
  - → Configure software
  - → Test system changes
  - → Approve system changes
  - → Deploy system changes
  - → Identify and evaluate system changes
  - → Identify changes in infrastructure, data, software, and procedures required to remediate incidents
  - → Create baseline configuration of IT technology
  - → Provide for changes necessary in emergency situations

CONTROL COMPONENT 9

Risk mitigation:

- [ ] **CC9.1: Identify, select, and develop risk mitigation activities for risks from potential business disruptions:**
  - → Consider mitigation of risks of business disruptions
  - → Consider the use of insurance to mitigate financial impact risks

- [ ] **CC9.2: Assess and manage risks associated with vendors and business partners:**
  - → Establish requirements for vendor and business partner engagements
  - → Assess vendor and business partner risks
  - → Assign responsibility and accountability for managing vendors and business partners
  - → Establish communication protocols for vendors and business partners
  - → Establish exception handling procedures from vendors and business partners
  - → Assess vendor and business partner performance
  - → Implement procedures for addressing issues identified during vendor and business partner assessments
  - → Implement procedures for terminating vendor and business partner relationships

---

There are additional principles and requirements that apply to the Trust Services Criteria of availability, processing integrity, privacy, and confidentiality, but those only apply as needed based on your organization.