# Documentation Checklist for SOC 2 Security Controls

Security program documentation establishes a foundation needed for organizations to effectively define and communicate control requirements. While critical to the success of a security program, keeping up with documentation requirements can be challenging for any organization. Whether you are just starting to develop a security program, or making continuous improvements to an established security program, this documentation checklist for SOC 2 Security Controls will help ensure that your organization maintains the appropriate documentation to support a successful security program. While this list may not be all inclusive for all organizations, you will likely need to account for these documents in some manner to achieve your compliance goals.

SOC 2 Security Controls are comprised of 18 control families. Each of the following sections contain the topics that should be addressed for each control family, followed by the recommended documentation that should be used to address them.

## 1. HARDWARE ASSET MANAGEMENT

Topics addressed by documentation for this control family should include:

1.1. Hardware Asset Inventory
1.2. Unauthorized Assets
1.3. Active Asset Discovery
1.4. Dynamic Host Configuration Protocol (DHCP) Logging
1.5. Passive Asset Discovery

Recommended documentation includes:

- ☐ **Hardware Asset Management Policy**
- ☐ **Hardware Asset Management Procedure**
- ☐ **Hardware Asset Inventory**
- ☐ Asset discovery tool reports
- ☐ Evidence of actions taken upon discovery of unauthorized assets
- ☐ Evidence of inventory review and updated every 6 months
- ☐ Evidence of active discovery tools configured to run at least daily

- [ ] Evidence of weekly log reviews and inventory updates
- [ ] Evidence of weekly reviews of DHCP logs
- [ ] Evidence of weekly reviews of passive discovery tool results
- [ ] Evidence of weekly reviews of unauthorized assets
- [ ] List of assets decommissioned by the organization
- [ ] List of authorized assets
- [ ] List of DHCP logging or IP address management tools
- [ ] List of new assets acquired by the organization
- [ ] List of passive discovery tools
- [ ] List of unauthorized assets

## 2. SOFTWARE ASSET MANAGEMENT

Topics addressed by documentation for this control family should include:

2.1. Software Asset Inventory
2.2. Vendor Supported Software
2.3. Unauthorized Software
2.4. Automated Software Inventory Tools
2.5. Whitelisting Authorized Software
2.6. Whitelisting Authorized Libraries
2.7. Whitelisting Authorized Scripts

Recommended documentation includes:

- [ ] **Software Asset Management Policy**
- [ ] **Software Asset Management Procedure**
- [ ] **Software Asset Inventory**

- [ ] Evidence of actions taken for unauthorized software without an approved exception
- [ ] Evidence of reviewing the unauthorized software list at least monthly
- [ ] Evidence of semi-annual re-assessment of the technical controls used to ensure only authorized software is used
- [ ] Evidence of semi-annual re-assessment of the technical controls used to ensure only authorized libraries are used
- [ ] Evidence of semi-annual re-assessment of the technical controls used to ensure only authorized scripts are used
- [ ] Evidence of semi-annual software asset inventory reviews
- [ ] Exception requests, if any, for unsupported software and the approval decision for each
- [ ] List of authorized software libraries
- [ ] List of authorized software scripts
- [ ] List of software inventory tools
- [ ] List of technical tools for ensuring only authorized libraries are used
- [ ] List of technical tools for ensuring only authorized software is used
- [ ] List of unsupported software with approved exceptions

## 3. DATA PROTECTION AND SECURITY PROGRAM

Topics addressed by documentation for this control family should include:

3.1. Data Protection and Security Program Management
3.2. Data Inventory
3.3. Data Access Control Lists
3.4. Data Retention

3.5. Secure Disposal of Data
3.6. Data Encryption on End User Devices
3.7. Data Classification Scheme
3.8. Data Flows
3.9. Data Encryption on Removable Media
3.10. Encryption of Data in Transit
3.11. Encryption of Data at Rest
3.12. Data Processing and Storage Segmentation
3.13. Data Loss Prevention
3.14. Data Access Logging

Recommended documentation includes:

- [ ] **Data Protection and Security Program Policy**
- [ ] **Data Protection and Security Program Procedure**
- [ ] **Data Inventory**
- [ ] Access control lists
- [ ] Data access control lists and permissions
- [ ] Data classification scheme
- [ ] Data encryption configuration details
- [ ] Data flow diagrams or documentation
- [ ] Data retention requirements
- [ ] Encryption configuration setting and associated documentation for data at rest
- [ ] Encryption configuration setting and associated documentation for data in transit
- [ ] Encryption configuration setting and associated documentation for removable media

- [ ] Evidence of annual documentation reviews and updates
- [ ] Evidence of annual reviews of the data inventory
- [ ] Evidence of annual security program documentation reviews and updates
- [ ] Evidence of data processing and storage segmentation
- [ ] Evidence of reviewing data flow diagrams at least annually
- [ ] Evidence of reviewing the data classification scheme at least annually
- [ ] List of automated tools used for data loss prevention
- [ ] List of data protection and security program documentation
- [ ] List of encrypted end user devices
- [ ] List of encrypted media
- [ ] List of minimum and maximum data retention requirements
- [ ] Sensitive data access logs

## 4. SECURE BASELINE CONFIGURATIONS

Topics addressed by documentation for this control family should include:

4.1. Hardware and Software Configurations
4.2. Network Infrastructure Configurations
4.3. Automatic Session Locking
4.4. Server Firewalls
4.5. End-User Device Firewalls
4.6. Secure Management of Hardware and Software
4.7. Default Accounts
4.8. Unnecessary Services
4.9. Trusted DNS Servers
4.10. Automatic Device Lockout
4.11. Remote Wipe Capability

4.12. Separate Organizational Workspaces

Recommended documentation includes:

- [ ] **Security Configuration Baseline Policy**
- [ ] **Security Configuration Baseline Procedure**
- [ ] Automatic device lockout configuration documentation for portable end user devices
- [ ] Configuration documentation for automatic session locking
- [ ] Configuration documentation for DNS servers
- [ ] Configuration documentation for the modification of default accounts
- [ ] Configuration documentation for uninstalling or disabling unnecessary services
- [ ] End user device configuration documentation for host-based firewalls
- [ ] Evidence of reviewing the secure hardware configuration documentation at least annually
- [ ] Evidence of reviewing the secure network infrastructure configuration documentation at least annually
- [ ] Evidence of reviewing the secure software configuration documentation at least annually
- [ ] List of all active accounts for all systems
- [ ] List of all disabled services for all systems
- [ ] List of all enabled services for all systems
- [ ] List of all inactive accounts for all systems
- [ ] List of authorized asset management protocols

- [ ] List of unauthorized asset management protocols
- [ ] Network diagram depicting firewall placements
- [ ] Secure hardware configuration documentation
- [ ] Secure network infrastructure configuration documentation
- [ ] Secure software configuration documentation

## 5. ACCOUNT MANAGEMENT

Topics addressed by documentation for this control family should include:

5.1. Inventory of Accounts
5.2. Unique Passwords
5.3. Inactive Accounts
5.4. Administrator Privilege Restrictions
5.5. Inventory of Service Accounts
5.6. Centralized Account Management

Recommended documentation includes:

- [ ] **Account Management Policy**
- [ ] **Account Management Procedure**
- [ ] Account inventory containing all accounts, including service accounts
- [ ] Configuration documentation for the directory or identity service used for centralized account management
- [ ] Evidence of quarterly verification of all privileged accounts
- [ ] Evidence of quarterly verification of all service accounts
- [ ] Evidence of quarterly verification of all user accounts
- [ ] Password composition and complexity requirements

## 6. ACCESS CONTROL

Topics addressed by documentation for this control family should include:

6.1. Access Provisioning
6.2. Access Revocation
6.3. Multi-Factor Authentication
6.4. Inventory of Authentication and Authorization Systems
6.5. Centralized Access Control
6.6. Role-Based Access Control

Recommended documentation includes:

- [ ] **Access Control Policy**
- [ ] **Access Control Procedure**
- [ ] Evidence that access control reviews are performed at least annually
- [ ] Evidence that reviews of the authentication and authorization system inventory are performed at least annually
- [ ] Inventory of authentication and authorization systems
- [ ] List of all external-facing applications
- [ ] List of all users with administrator or elevated access privileges
- [ ] List of all users with remote access privileges
- [ ] List of recently onboarded personnel
- [ ] List of recently terminated or separated personnel
- [ ] Multi-factor authentication configuration settings and associated documentation for administrator or elevated access
- [ ] Multi-factor authentication configuration settings and associated documentation for each external-facing application

- [ ] Multi-factor authentication configuration settings and associated documentation for remote access
- [ ] Role-based access control (RBAC) matrix

## 7. VULNERABILITY MANAGEMENT

Topics addressed by documentation for this control family should include:

7.1. Vulnerability Management Process
7.2. Vulnerability Remediation Process
7.3. Patch Management
7.4. Vulnerability Scanning
7.5. Remediation of Detected Vulnerabilities

Recommended documentation includes:

- [ ] **Vulnerability Management Policy**
- [ ] **Vulnerability Management Procedure**
- [ ] Evidence of annual vulnerability management process reviews and updates
- [ ] Evidence of compliance with vulnerability remediation timelines
- [ ] Evidence of monthly patch management processes being performed
- [ ] Evidence of monthly vulnerability remediation reviews
- [ ] Monthly automated vulnerability scan results for credentialed scans performed on external-facing assets
- [ ] Monthly automated vulnerability scan results for non-credentialed scans performed on external-facing assets
- [ ] Quarterly automated vulnerability scan results for credentialed scans performed on internal assets
- [ ] Quarterly automated vulnerability scan results for non-credentialed scans performed on internal assets

- [ ] Risk-based vulnerability remediation strategy

## 8. AUDIT LOG MANAGEMENT

Topics addressed by documentation for this control family should include:

8.1. Audit Log Management Process
8.2. Audit Log Collection
8.3. Audit Log Storage
8.4. Standardized Time Synchronization
8.5. Detailed Audit Logs
8.6. DNS Query Audit Logs
8.7. URL Request Audit Logs
8.8. Command Line Audit Logs
8.9. Centralized Audit Logs
8.10. Audit Log Retention
8.11. Audit Log Reviews
8.12. Service Provider Logs

Recommended documentation includes:

- [ ] **Audit Log Management Policy**
- [ ] **Audit Log Management Procedure**
- [ ] Audit log retention configuration settings
- [ ] Audit log storage configurations and status
- [ ] Audit logging configuration settings for systems containing sensitive data
- [ ] Centralized audit log configuration settings and associated documentation
- [ ] Evidence of annual audit log management process reviews and updates
- [ ] Evidence of weekly audit log reviews
- [ ] List of DNS servers

- [ ] List of service provider logs that are collected for authentication, data creation or disposal, and user access management
- [ ] List of system containing sensitive data
- [ ] List of time synchronization sources
- [ ] System-generated audit logs
- [ ] System-generated DNS query audit logs
- [ ] System-generated logs of command line activities
- [ ] System-generated logs of URL requests
- [ ] System time synchronization configuration settings and associated documentation

## 9. EMAIL AND INTERNET SECURITY

Topics addressed by documentation for this control family should include:

9.1. Fully Supported Web Browsers and Email Clients
9.2. DNS Filtering Services
9.3. Network Based URL Filters
9.4. Unauthorized Browser and Email Client Extensions
9.5. DMARC Records
9.6. Unnecessary File Types
9.7. Email Server Anti-Malware Protection

Recommended documentation includes:

- [ ] **Email and Internet Security Policy**
- [ ] **Email and Internet Security Procedure**
- [ ] Configuration settings and associated documentation for email anti-malware protection, such as attachment scanning and sandboxing
- [ ] Configuration settings for Domain Keys Identified Mail (DKIM)

- [ ] Configuration settings for Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- [ ] Configuration settings for Sender Policy Framework (SPF)
- [ ] Configuration settings for the installed versions of email clients
- [ ] Configuration settings for the installed versions of web browsers
- [ ] DNS filtering service configuration settings
- [ ] Email configuration settings and associated documentation for blocking unnecessary file types
- [ ] List of known malicious domains
- [ ] Network-based URL filtering configuration settings and associated documentation

## 10. MALWARE PREVENTION

Topics addressed by documentation for this control family should include:

10.1. Anti-Malware Software
10.2. Anti-Malware Signature Updates
10.3. Removable Media Auto-run and Auto-play
10.4. Automatic Scanning of Removable Media
10.5. Anti-Exploitation Features
10.6. Central Management of Anti-Malware Software
10.7. Behavior Based Anti-Malware Software

Recommended documentation includes:

- [ ] **Malware Prevention Policy**
- [ ] **Malware Prevention Procedure**
- [ ] Configuration settings and associated documentation for anti-exploitation features

- [ ] Configuration settings and associated documentation for automatically scanning removable media
- [ ] Configuration settings and associated documentation for disabling auto-run, auto-play, and auto-execute functionality for removable media
- [ ] Configuration settings and associated documentation for the centralized management of anti-malware software
- [ ] List of information assets
- [ ] System-generated report showing installed version of malware protection and date of last update
- [ ] System-generated report showing the list of information assets with malware protection

## 11. DATA RECOVERY

Topics addressed by documentation for this control family should include:

11.1. Data Recovery Process
11.2. Automated Backups
11.3. Protection of Recovery Data
11.4. Isolated Instance of Recovery Data
11.5. Data Recovery Testing

Recommended documentation includes:

- [ ] **Data Recovery Policy**
- [ ] **Data Recovery Procedure**
- [ ] Configuration settings and associated documentation for automated backups
- [ ] Encryption configuration settings for backup data
- [ ] Evidence of annual data recovery process documentation reviews and updates

- [ ] Evidence of backups being performed at least weekly
- [ ] Evidence of isolated data backups for critical data
- [ ] Evidence of quarterly data recovery testing

## 12. NETWORK INFRASTRUCTURE MANAGEMENT

Topics addressed by documentation for this control family should include:

12.1. Keeping Network Infrastructure Up to Date
12.2. Secure Network Architecture
12.3. Secure Network Infrastructure Management
12.4. Architecture Diagrams
12.5. Network Authentication, Authorization, and Auditing (AAA)
12.6. Network Management and Communication Protocols
12.7. Connecting to the AAA Infrastructure
12.8. Dedicated Computing Resources for Administrator Work

Recommended documentation includes:

- [ ] **Network Infrastructure Management Policy**
- [ ] **Network Infrastructure Management Procedure**
- [ ] Architecture diagrams
- [ ] Configuration settings and associated documentation for secure network architecture, including segmentation, least privileges, and availability requirements
- [ ] Evidence of annual architecture diagram reviews and updates
- [ ] Evidence of monthly software version reviews to verify implemented software remains supported
- [ ] Evidence of network infrastructure being kept up to date
- [ ] Evidence of physical or logical separation of computing resources used for administrator-level activities

- [ ] List of network management and communication protocols
- [ ] List of protocols that are enabled for managing the network infrastructure

## 13. NETWORK MONITORING AND DEFENSE

Topics addressed by documentation for this control family should include:

13.1. Centralized Security Event Alerting
13.2. Host Based Intrusion Detection
13.3. Network Based Intrusion Detection
13.4. Traffic Filtering between Network Segments
13.5. Access Controls for Remote Assets
13.6. Network Traffic Flow Logs
13.7. Host Based Intrusion Prevention
13.8. Network Based Intrusion Prevention
13.9. Port Level Access Controls
13.10. Application Layer Filtering
13.11. Security Event Alert Threshold Tuning

Recommended documentation includes:

- [ ] **Network Monitoring and Defense Policy**
- [ ] **Network Monitoring and Defense Procedure**
- [ ] Configuration settings and associated documentation for application layer filtering
- [ ] Configuration settings and associated documentation for host-based intrusion detection
- [ ] Configuration settings and associated documentation for host-based intrusion prevention
- [ ] Configuration settings and associated documentation for network-based intrusion detection

- [ ] Configuration settings and associated documentation for network-based intrusion prevention
- [ ] Configuration settings and associated documentation for port-level access controls
- [ ] Configuration settings and associated documentation for the centralized management of security event logging and alerting
- [ ] Configuration settings and associated documentation for verifying the security of assets connecting remotely
- [ ] Evidence of monthly reviews and updates of event alerting thresholds
- [ ] List of assets on which host-based intrusion detection is implemented
- [ ] List of assets on which host-based intrusion prevention is implemented
- [ ] List of security event alerting thresholds
- [ ] Network flow logs

## 14. SECURITY AWARENESS TRAINING

Topics addressed by documentation for this control family should include:

14.1. Security Awareness Training Program
14.2. Social Engineering Attacks
14.3. Authentication Best Practices
14.4. Data Handling Best Practices
14.5. Unintentional Data Exposure
14.6. Recognizing and Reporting Security Incidents
14.7. Missing Security Updates Identification and Reporting
14.8. Dangers of Insecure Networks
14.9. Role-Based Security Awareness Training

Recommended documentation includes:

- [ ] **Security Awareness Training Policy**

- [ ] **Security Awareness Training Procedure**
- [ ] Evidence of annual security awareness training content reviews and updates
- [ ] List of recently hired personnel
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training records

## 15. THIRD-PARTY DUE DILIGENCE

Topics addressed by documentation for this control family should include:

15.1. Inventory of Third Parties
15.2. Third-Party Classification
15.3. Contractual Security Requirements
15.4. Assessing Third Parties
15.5. Monitoring Third Party Services
15.6. Ending Third-Party Relationships

Recommended documentation includes:

- [ ] **Third-Party Due Diligence Policy**
- [ ] **Third-Party Due Diligence Procedure**
- [ ] Assigned classification tiers for existing inventory of third parties
- [ ] Classification tiers of third-party providers and suppliers
- [ ] Contractual security requirements
- [ ] Evidence of annual third-party classification tier reviews and updates
- [ ] Evidence of annual third-party inventory reviews and updates
- [ ] Evidence of annual third-party provider contract reviews

- [ ] Evidence of annual third-party provider due diligence assessments / re-assessments
- [ ] Inventory of all third-party providers and suppliers
- [ ] Results of third-party due diligence assessments
- [ ] Third-party due diligence assessment materials
- [ ] Third-party provider monitoring results

## 16. APPLICATION SECURITY

Topics addressed by documentation for this control family should include:

16.1. Secure Application Development Process
16.2. Addressing Software Vulnerabilities
16.3. Root Cause Analysis for Vulnerabilities
16.4. Inventory of Third-Party Software Components
16.5. Trusted Third-Party Software Components
16.6. Severity Rating System for Vulnerabilities
16.7. Standard Hardening Configuration Templates
16.8. Separation of Production and Non-Production Systems
16.9. Secure Coding Training for Developers
16.10. Secure Design Principles
16.11. Application Security Components
16.12. Code Level Security Checks
16.13. Application Penetration Testing
16.14. Threat Modeling

Recommended documentation includes:

- [ ] **Application Security Policy**
- [ ] **Application Security Procedure**
- [ ] Application penetration testing results

- [ ] Evidence of root cause analysis being performed on identified application security vulnerabilities
- [ ] Evidence of separate environments for production and non-production systems
- [ ] Evidence that application develop documentation is reviewed and updated at least annually
- [ ] Evidence that the inventory of third-party software component inventory is reviewed and updated at least monthly
- [ ] Evidence that the severity rating system for application vulnerabilities is reviewed and updated at least annually
- [ ] Inventory of third-party software components
- [ ] List of application and system developers
- [ ] List of application infrastructure components
- [ ] List of static and dynamic analysis tools
- [ ] Secure coding training curriculum
- [ ] Secure coding training materials
- [ ] Secure coding training records
- [ ] Secure design principles
- [ ] Severity rating system for application vulnerabilities
- [ ] Standard hardening configuration templates
- [ ] System-generate configuration settings report for application infrastructure components
- [ ] Threat modeling criteria and results

## 17. INCIDENT RESPONSE

Topics addressed by documentation for this control family should include:

17.1. Incident Handling
17.2. Contact Information for Reporting Security Incidents
17.3. Incident Reporting Process
17.4. Incident Response Process
17.5. Key Roles and Responsibilities
17.6. Communications During Incident Response
17.7. Incident Response Exercises
17.8. Post-Incident Reviews
17.9. Security Incident Thresholds

Recommended documentation includes:

- [ ] **Incident Response Policy**
- [ ] **Incident Response Procedure**
- [ ] **Incident Response Plan**
- [ ] Contact information for incident response personnel and participants
- [ ] Evidence of annual Incident Response Plan reviews and updates
- [ ] Evidence that contacts and contact information is reviewed and updated at least annually
- [ ] Evidence that incident response roles and responsibilities are reviewed and updated at least annually
- [ ] Evidence that primary and secondary incident response communication mechanisms are reviewed and updated at least annually
- [ ] Evidence that security incident thresholds are reviewed and updated at least annually
- [ ] Lessons learned meeting agenda and minutes
- [ ] List of incident handlers

- [ ] List of incident response exercises and scenarios
- [ ] List of primary and secondary incident response communication mechanisms
- [ ] List of security incident thresholds
- [ ] Results of annual incident response exercises and scnenarios

**18. PENETRATION TESTING**

Topics addressed by documentation for this control family should include:

18.1. Penetration Testing Program
18.2. External Penetration Tests
18.3. Remediation of Findings
18.4. Security Measure Validation
18.5. Internal Penetration Tests

Recommended documentation includes:

- [ ] **Penetration Testing Policy**
- [ ] **Penetration Testing Procedure**
- [ ] External penetration testing reports
- [ ] Internal penetration testing reports
- [ ] Penetration test remediation results
- [ ] Results of rulesets and security measure reviews, post testing

**About ASCENT:** The ASCENT Portal is a secure cloud-based system of record that supports the lifecycle management of security program controls and the resulting continuous compliance for organizations of any size, in any industry. As the single source of security and compliance truth, the ASCENT Portal puts everything you need to comply with security control requirements right at your fingertips. From security assessments and calendar-driven control task reminders to governance documentation and vendor management, ASCENT automates your compliance process, end-to-end, while delivering real-time status and reports all from a single source. Visit ascent-portal.com to schedule a demo focused on making the ASCENT to your security and continuous compliance goals.

Don't become overwhelmed by documentation. If you have a question about security program documentation, you can schedule a free 15-minute consultative discussion by clicking here. You do not need to be an ASCENT Portal customer to take advantage of this no-cost opportunity.