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 NIST SP 800-171 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.

NIST SP 800-171 is comprised of 14 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. ACCESS CONTROL

Topics addressed by documentation for this control family should include:

1.1. Access Management
1.2. Controlling Access to Transactions and Functions
1.3. Controlling the Flow of Information
1.4. Segregation of Duties
1.5. Least Privilege Principle
1.6. Using Non-Privileged Accounts Versus Privileged Accounts
1.7. Logging the Use of Privileged Functions
1.8. Unsuccessful Logon Attempts
1.9. Logon Banners and/or System Use Notifications
1.10. Session Locks
1.11. Terminating Sessions
1.12. Remote Access Management
1.13. Confidentiality of Remote Access
1.14. Remote Access Control Points
1.15. Remote Access to Privileged Function and Information
1.16. Authorizing Wireless Access
1.17. Wireless Access Protections
1.18. Mobile Device Connections
1.19. Mobile Device Encryption

1.20. Connections to External Systems
1.21. Portable Storage Devices on External Systems
1.22. Managing Publicly Accessible Content

Recommended documentation includes:

- [ ] **Access Control Policy**
- [ ] **Access Control Procedure**
- [ ] Access authorization records
- [ ] Account management compliance reviews
- [ ] Authorizations for mobile device connections to organizational systems
- [ ] Description of encryption mechanisms and associated configurations
- [ ] Documented approval of system user notification messages or banners
- [ ] List of active system accounts and the name of the associated used for each
- [ ] List of all managed network access control points
- [ ] List of internal applications accessible from external systems
- [ ] List of approved authorizations, including remote access authorizations
- [ ] List of conditions for group and role membership
- [ ] List of conditions or trigger events requiring session disconnections
- [ ] List of devices and systems authorized to connect to information systems controlled by the organization
- [ ] List of divisions of responsibility and separation of duties
- [ ] List of information flow authorizations
- [ ] List of privileged functions and associated user account assignments

- [ ] List of recently disabled accounts and the name of the associated user
- [ ] List of security functions and security relevant information for which access is to be explicitly authorized
- [ ] List of system administration personnel
- [ ] List of users authorized to publish publicly accessible content
- [ ] Notifications or records of recently transfer or terminated personnel.
- [ ] Records of publicly accessible information reviews
- [ ] Records of response to non-public information discovered on public websites
- [ ] Remote access authorizations
- [ ] Security awareness training records
- [ ] System access authorizations
- [ ] System audit logs and records
- [ ] System baseline configurations
- [ ] System configuration settings and associated documentation
- [ ] System Connection or Processing Agreements
- [ ] System Design Documentation
- [ ] System-generated list of privileged accounts
- [ ] System-generated list of security functions assigned to accounts or roles
- [ ] System monitoring and audit records
- [ ] System Security Plan
- [ ] System use notification or logon banner messages

- [ ] Terms and conditions for external systems
- [ ] Training materials and records
- [ ] User acknowledgements of system use notification or logon banner
- [ ] Wireless access authorizations

2. SECURITY AWARENESS TRAINING

Topics addressed by documentation for this control family should include:

2.1. Security Awareness Training for All Personnel
2.2. Role-Based Security Awareness Training
2.3. Insider Threat Awareness Training

Recommended documentation includes:

- [ ] **Security Awareness Training Policy**
- [ ] **Security Awareness Training Procedure**
- [ ] Relevant codes of federal regulations
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training records
- [ ] System Security Plan

3. AUDIT AND ACCOUNTABILITY

Topics addressed by documentation for this control family should include:

3.1. System Audit Logging
3.2. User Accountability
3.3. Reviewing and Updating Types of Logged Events
3.4. Audit Log Failures

3.5. Correlation of Audit Record Review, Analysis, and Reporting
3.6. Audit Record Retention and Report Generation
3.7. Authoritative Time Source
3.8. Audit Log Protection
3.9. Access Limitations for Audit Management

Recommended documentation includes:

- [ ] **Audit and Accountability Policy**
- [ ] **Audit and Accountability Procedure**
- [ ] Access authorizations
- [ ] Access control lists
- [ ] List of audit logging tools
- [ ] List of audit record reduction, review, analysis, and reporting tools
- [ ] List of the event types that are to be logged
- [ ] List of personnel to be notified in the event of an audit logging failure
- [ ] List of system auditable events
- [ ] Records of the list of event types to be logged being reviewed and updated
- [ ] Reports of audit findings
- [ ] System audit logs and record across different repositories
- [ ] System configuration settings and associated documentation
- [ ] System design documentation
- [ ] System events
- [ ] System incident reports

☐ System Security Plan

☐ System-generated list of privileged users with access needed for managing audit logging functionality

4. CONFIGURATION MANAGEMENT

Topics addressed by documentation for this control family should include:

4.1. Baseline Configurations
4.2. Security Configuration Settings and Enforcement
4.3. Change Control Management
4.4. Security Impact Analysis
4.5. Access Restrictions for Implementing Changes
4.6. Principle of Least Functionality
4.7. Controlling Non-Essential Functionality
4.8. Software Whitelisting and Blacklisting
4.9. User Installed Software

Recommended documentation includes:

☐ **Configuration Management Policy**

☐ **Configuration Management Procedure**

☐ **Configuration Management Plan**

☐ Agenda or minutes from configuration change control meetings

☐ Baseline configurations

☐ Change control audit and review reports

☐ Change control records

☐ Continuous monitoring strategy

☐ Documented reviews of programs, functions, ports, protocols, and services

☐ Enterprise architecture documentation

- [ ] Evidence supporting approved deviations from approved configurations
- [ ] Inventory review and update records
- [ ] List of access credentials
- [ ] List of analysis tools and associated outputs
- [ ] List of rules governing user-installed software
- [ ] List of software programs authorized to execute on systems
- [ ] List of software programs not authorized to execute on systems
- [ ] Logical access approvals
- [ ] Physical access approvals
- [ ] Records of authorized and unauthorized software list reviews and updates
- [ ] Security configuration checklists
- [ ] Security impact analysis documentation
- [ ] Specifications for preventing software program execution
- [ ] System architecture and configuration documentation
- [ ] System audit logs and records
- [ ] System component installation records
- [ ] System component removal records
- [ ] System configuration settings and associated documentation
- [ ] System design documentation
- [ ] System inventory records

- [ ] System monitoring records
- [ ] System Security Plan

5. IDENTIFICATION AND AUTHENTICATION

Topics addressed by documentation for this control family should include:

5.1. Identification of Users, Processes, and Devices
5.2. Authentication of Users, Processes, and Devices
5.3. Multi-Factor Authentication
5.4. Replay-Resistant Authentication
5.5. Re-Use of Identifiers or Accounts
5.6. Identifier or Account Inactivity
5.7. Password Complexity
5.8. Password History
5.9. Temporary Passwords
5.10. Protecting Password with Cryptography
5.11. Obscuring Authentication Feedback

Recommended documentation includes:

- [ ] **Identification and Authentication Policy**
- [ ] **Identification and Authentication Procedure**
- [ ] Change control records associated with managing system authenticators
- [ ] List of system accounts
- [ ] List of system authenticator types
- [ ] System configuration settings and associated documentation
- [ ] System design documentation
- [ ] System Security Plan

6. INCIDENT RESPONSE

Topics addressed by documentation for this control family should include:

6.1. Incident Handling
6.2. Incident Tracking and Reporting
6.3. Incident Response Testing

Recommended documentation includes:

- [ ] **Incident Response Policy**
- [ ] **Incident Response Procedure**
- [ ] **Incident Response Plan**
- [ ] Incident reporting records and documentation
- [ ] Incident response records and documentation
- [ ] Incident response test plan
- [ ] Incident response test results
- [ ] Incident response testing materials
- [ ] Incident response training curriculum
- [ ] Incident response training materials
- [ ] Incident response training records
- [ ] System Security Plan

7. SYSTEM AND DEVICE MANAGEMENT

Topics addressed by documentation for this control family should include:

7.1. Performing Maintenance
7.2. Controlling Maintenance
7.3. Equipment Sanitization

7.4. Maintenance Media Inspection
7.5. Non-Local Maintenance
7.6. Supervising Maintenance Personnel

Recommended documentation includes:

- [ ] **System Maintenance Policy**
- [ ] **System Maintenance Procedure**
- [ ] Access control records
- [ ] Diagnostic records
- [ ] Equipment sanitization records
- [ ] List of authorized personnel
- [ ] List of system maintenance tools and associated documentation
- [ ] Maintenance records
- [ ] Maintenance tools inspection records
- [ ] Manufacturer or vendor maintenance specifications
- [ ] Media sanitization records
- [ ] Service level agreements
- [ ] Service provider contracts
- [ ] System configuration settings and associated documentation
- [ ] System design documentation
- [ ] System Security Plan

8. MEDIA PROTECTION

Topics addressed by documentation for this control family should include:

8.1. Media Storage
8.2. Media Access
8.3. Media Sanitization and Destruction
8.4. Media Marking
8.5. Media Transport
8.6. Media Encryption
8.7. Use of Removable Media
8.8. Portable Storage Devices
8.9. Backup Media Security

Recommended documentation includes:

- [ ] **Media Protection Policy**
- [ ] **Media Protection Procedure**
- [ ] Backup storage locations
- [ ] List and locations of designated controlled areas
- [ ] List and locations of media storage facilities
- [ ] List of media
- [ ] List of media marking security attributes
- [ ] Media sanitization records
- [ ] Media transport records
- [ ] Rules of behavior
- [ ] System audit logs and records
- [ ] System backup logs or records
- [ ] System configuration settings and associated documentation

- [ ] System design documentation
- [ ] System Security Plan

9. PERSONNEL SECURITY

Topics addressed by documentation for this control family should include:

9.1. Personnel Screening
9.2. Personnel Transfers and Terminations

Recommended documentation includes:

- [ ] **Personnel Security Policy**
- [ ] **Personnel Security Procedure**
- [ ] Exit interview records
- [ ] Personnel transfer and termination activity records
- [ ] Personnel screening records
- [ ] Terminated or revoked authenticators and credential records
- [ ] System Security Plan

10. PHYSICAL SECURITY

Topics addressed by documentation for this control family should include:

10.1. Physical Access Limitations
10.2. Facility Protection and Monitoring
10.3. Escorting and Monitoring Visitors
10.4. Physical Access Logs
10.5. Physical Access Devices
10.6. Alternate Work Sites

Recommended documentation includes:

- [ ] **Physical Security Policy**

- [ ] **Physical Security Procedure**
- [ ] Access control records
- [ ] Assessments of safeguards at alternate sites
- [ ] Authorized personnel access lists
- [ ] Inventory records of physical access control devices
- [ ] List of authorization credentials
- [ ] List of safeguards required for alternate work sites
- [ ] List of security safeguards that control access to designated publicly accessible areas within facilities
- [ ] List of system accounts
- [ ] List of entry and exit points
- [ ] Physical access list reviews
- [ ] Physical access logs or records
- [ ] Physical access monitoring records
- [ ] Physical access termination records and associated documentation
- [ ] Records of key and lock combination changes
- [ ] Records of physical access logs reviews
- [ ] Storage locations for physical access control devices
- [ ] System Security Plan

11. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

11.1. Performing Risk Assessments
11.2. Vulnerability Monitoring and Scanning
11.3. Vulnerability Remediation

Recommended documentation includes:

- [ ] **Risk Management Policy**
- [ ] **Risk Management Procedure**
- [ ] Patch and vulnerability management records
- [ ] Records of risk assessment reviews
- [ ] Risk assessment
- [ ] Risk assessment results
- [ ] Risk assessment updates
- [ ] Security assessment report
- [ ] System Security Plan
- [ ] Vulnerability scanning results
- [ ] Vulnerability scanning tools and associated configuration documentation

12. SECURITY PROGRAM ASSESSMENTS

Topics addressed by documentation for this control family should include:

12.1. Security Control Assessments
12.2. Plan of Actions and Milestones
12.3. Continuous Monitoring
12.4. System Security Plans

Recommended documentation includes:

- [ ] **Security Program Assessment Policy**
- [ ] **Security Program Assessment Procedure**
- [ ] Enterprise architecture documentation
- [ ] Plans of action
- [ ] Records of System Security Plan reviews and updates
- [ ] Security assessment evidence
- [ ] Security assessment plan
- [ ] Security assessment report
- [ ] System Security Plan

13. SYSTEMS AND COMMUNICATIONS SECURITY

Topics addressed by documentation for this control family should include:

13.1. Boundary Protection
13.2. Security Designs, Techniques, and Principles
13.3. Separation of User and System Functionality
13.4. Securing Shared System Resources
13.5. Publicly Accessible System Components
13.6. Network Communications Traffic
13.7. Split Tunneling
13.8. Protecting Data in Transit
13.9. Connection Terminations
13.10. Key Management
13.11. FIPS Validated Encryption
13.12. Collaborative Device Control
13.13. Mobile Code Control
13.14. VoIP Technologies
13.15. Session Authenticity
13.16. Protecting Data at Rest

Recommended documentation includes:

- [ ] **Systems and Communications Security Policy**
- [ ] **Systems and Communications Security Procedure**
- [ ] Cryptographic module validation certificates
- [ ] Description of cryptographic mechanisms and associated configuration documentation
- [ ] Enterprise architecture documentation
- [ ] Enterprise security architecture documentation
- [ ] List of acceptable mobile code and mobile code technologies
- [ ] List of boundary protection hardware and software
- [ ] List of FIPS-validated cryptographic modules
- [ ] List of information at rest that requires confidentiality protections
- [ ] List of key internal boundaries of systems
- [ ] List of unacceptable mobile code and mobile technologies
- [ ] Mobile code implementation controls and processes
- [ ] Mobile code usage restrictions
- [ ] Records of System Security Plan reviews and updates
- [ ] Security architecture documentation
- [ ] Security requirements and specification for information systems
- [ ] System architecture and configuration documentation
- [ ] System audit logs and records

- [ ] System hardware and software inventories
- [ ] System monitoring records
- [ ] System Security Plan
- [ ] VoIP implementation guidance
- [ ] VoIP usage restrictions

14. SYSTEM AND INFORMATION INTEGRITY

Topics addressed by documentation for this control family should include:

14.1. Flaw Remediation
14.2. Malicious Code Protection
14.3. Responding to Security Alerts and Advisories
14.4. Malicious Code Protection Updates
14.5. System and File Scanning
14.6. Monitoring Systems for Attacks
14.7. Unauthorized Use Monitoring

Recommended documentation includes:

- [ ] **System and Information Integrity Policy**
- [ ] **System and Information Integrity Procedure**
- [ ] Continuous monitoring strategy
- [ ] Facility diagram or layout
- [ ] Installation or change control records for security-relevant software and firmware updates
- [ ] List of flaws and vulnerabilities potentially affecting information systems
- [ ] List of locations within systems where monitoring devices are deployed
- [ ] List of malicious code protection mechanisms

- [ ] List of recent security flaw remediation actions preformed on systems
- [ ] List of system protocols
- [ ] Records of actions initiated by malicious code protection mechanisms
- [ ] Records of malicious code protection updates
- [ ] Records of security alerts and advisories
- [ ] Scan results from malicious code protection mechanisms
- [ ] System audit logs and records
- [ ] System configuration settings and associated documentation
- [ ] System design documentation
- [ ] System monitoring tools and techniques documentation
- [ ] System Security Plan
- [ ] Test results after installing updates to correct system flaws

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.