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 800-53 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 800-53 is comprised of 20 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. Policy and Procedure
1.2. Account Management
1.3. Access Enforcement
1.4. Information Flow Enforcement
1.5. Separation of Duties
1.6. Least Privilege
1.7. Unsuccessful Logon Attempts
1.8. Logon banners and System Use Notification
1.9. Device Locks
1.10. Session Termination
1.11. Permitted Actions without Identification or Authentication
1.12. Remote Access
1.13. Wireless Access
1.14. Mobile Device Access Control
1.15. Use of External Systems
1.16. Information Sharing
1.17. Publicly Accessible Content

Recommended documentation includes:

- [ ] **Access Control Policy**
- [ ] **Access Control Procedure**
- [ ] Control Evidence Document for each Access Control defined control
- [ ] List of all personnel
- [ ] List of all accounts
- [ ] List of recently terminated personnel
- [ ] List of recently onboarded personnel
- [ ] List of disabled accounts for high-risk users
- [ ] Data flow diagrams
- [ ] Separation of duties matrix
- [ ] List of privileged accounts
- [ ] Record of user access and privilege reviews
- [ ] System-generated logs for privileged account activities
- [ ] System-generated reports of unsuccessful logon attempts
- [ ] Logon banners and system use notifications
- [ ] List of permitted actions without identification or authentication, if applicable
- [ ] List of users with remote access permissions
- [ ] Remote access monitoring records
- [ ] Encryption configuration settings for remote access
- [ ] Inventory of remote access control points

- [ ] List of authorized privileged commands and data access via remote access
- [ ] List of users with wireless access
- [ ] Inventory of wireless access points
- [ ] Wireless access authentication and encryption configurations
- [ ] List of users authorized to use mobile devices
- [ ] Mobile device encryption configuration settings
- [ ] Records for reviews of publicly available content

2. SECURITY AWARENESS TRAINING PROGRAM

Topics addressed by documentation for this control family should include:

2.1. Policy and Procedure
2.2. Security Awareness Training
2.3. Role-Based Security Awareness Training
2.4. Training Records

Recommended documentation includes:

- [ ] **Security Awareness Training Program Policy**
- [ ] **Security Awareness Training Program Procedure**
- [ ] Control Evidence Document for each Security Awareness Training Program defined control
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training schedule
- [ ] Security awareness training records

3. AUDIT AND ACCOUNTABILITY

Topics addressed by documentation for this control family should include:

3.1. Policy and Procedure
3.2. Event Logging
3.3. Content of Audit Records
3.4. Audit Log Storage Capacity
3.5. Responding to Audit Logging Process Failures
3.6. Audit Record Review, Analysis, and Reporting
3.7. Audit Record Reduction and Report Generation
3.8. Time Stamps
3.9. Protection of Audit Log Records
3.10. Audit Record Retention
3.11. Audit Record Generation

Recommended documentation includes:

- [ ] **Audit and Accountability Policy**
- [ ] **Audit and Accountability Procedure**
- [ ] Control Evidence Document for each Audit and Accountability defined control
- [ ] List of event types that are logged for information systems and devices
- [ ] Record from reviews of type of events being logged
- [ ] Records of responding to audit logging process failures
- [ ] Records of audit record reviews, analysis, and reporting
- [ ] Audit record retention schedule

4. ASSESSMENT, AUTHORIZATION, AND MONITORING

Topics addressed by documentation for this control family should include:

4.1. Policy and Procedure
4.2. Security Program Control Assessments
4.3. Information Exchange

4.4. Plan of Action and Milestones
4.5. Authentication of Information Systems
4.6. Continuous Monitoring
4.7. Internal System Connections

Recommended documentation includes:

- [ ] **Assessment, Authorization, and Monitoring Policy**
- [ ] **Assessment, Authorization, and Monitoring Procedure**
- [ ] Control Evidence Document for each Assessment, Authorization, and Monitoring defined control
- [ ] Security Program control assessment results
- [ ] Plan of Actions and Milestones (POAMs)
- [ ] Record of POAM reviews
- [ ] Continuous Monitoring Plan
- [ ] Risk Monitoring Plan
- [ ] List of internal system connections

5. CONFIGURATION MANAGEMENT

Topics addressed by documentation for this control family should include:

5.1. Policy and Procedure
5.2. Baseline Configurations
5.3. Configuration Change Control
5.4. Security Impact Analysis
5.5. Access Restrictions for Making Changes
5.6. Configuration Settings
5.7. Least Functionality
5.8. System Component Inventory
5.9. Configuration Management Plan
5.10. Software Usage Restrictions

5.11. User-Installed Software
5.12. Information Locations

Recommended documentation includes:

- [ ] **Configuration Management Policy**
- [ ] **Configuration Management Procedure**
- [ ] Control Evidence Document for each Configuration Management defined control
- [ ] System and device baseline configuration settings
- [ ] System configuration settings for high-risk areas
- [ ] Configuration change control requests and approval decisions
- [ ] Security impact analysis results for requested changes
- [ ] Access permissions authorized for making changes
- [ ] Records of system functionality reviews to support least-privilege principle
- [ ] List of authorized software
- [ ] System component inventory
- [ ] List of recently installed system components or devices
- [ ] List of recently decommissioned or uninstalled system components or devices
- [ ] Records of response actions taken upon detecting unauthorized components
- [ ] Configuration management plan

6. CONTINGENCY PLANNING

Topics addressed by documentation for this control family should include:

6.1. Policy and Procedure

6.2. Contingency Plan
6.3. Contingency Plan Training
6.4. Contingency Plan Testing
6.5. Alternate Storage Site(s)
6.6. Alternate Processing Site(s)
6.7. Telecommunications Services
6.8. System Backups
6.9. System Recovery and Reconstitution

Recommended documentation includes:

- [ ] **Contingency Planning Policy**
- [ ] **Contingency Planning Procedure**
- [ ] Control Evidence Document for each Contingency Planning defined control
- [ ] Contingency plans
- [ ] Business impact analysis results
- [ ] List of critical systems and functions
- [ ] Contingency plan training materials and training records
- [ ] Contingency plan test scripts
- [ ] Contingency plan testing reports
- [ ] Name and location of alternate storage site(s)
- [ ] Name and location of alternate processing site(s)
- [ ] System backup schedule
- [ ] Record of data backup recovery testing

7. IDENTIFICATION AND AUTHENTICATION

Topics addressed by documentation for this control family should include:

7.1. Policy and Procedure
7.2. Identification and Authentication for Internal Users
7.3. Device Identification and Authentication
7.4. Identifier Management
7.5. Authenticator Management
7.6. Authentication Feedback
7.7. Cryptographic Module Authentication
7.8. Identification and Authentication for External Users
7.9. Re-Authentication
7.10. Identity Proofing

Recommended documentation includes:

- [ ] **Identification and Authentication Policy**
- [ ] **Identification and Authentication Procedure**
- [ ] Control Evidence Document for each Identification and Authentication defined control
- [ ] Multi-factor authentication configuration settings for privileged accounts
- [ ] Multi-factor authentication configuration settings for non-privileged accounts
- [ ] Multi-factor authentication configuration settings for remote access
- [ ] List of approved PIV credentials, if applicable

8. INCIDENT RESPONSE

Topics addressed by documentation for this control family should include:

8.1. Policy and Procedure
8.2. Incident Response Training
8.3. Incident Response Testing
8.4. Incident Handling
8.5. Incident Monitoring

8.6. Incident Reporting
8.7. Incident Response Assistance
8.8. Incident Response Plan

Recommended documentation includes:

- [ ] **Incident Response Policy**
- [ ] **Incident Response Procedure**
- [ ] Control Evidence Document for each Incident Response defined control
- [ ] Incident response training materials and training records
- [ ] Incident response training materials and training records
- [ ] Incident response test scripts
- [ ] Incident response testing report
- [ ] Incident reports
- [ ] Incident Response Plan

9. SYSTEM AND DEVICE MANAGEMENT

Topics addressed by documentation for this control family should include:

9.1. Policy and Procedures
9.2. Controlled Maintenance
9.3. Maintenance Tools
9.4. Nonlocal Maintenance
9.5. Maintenance Personnel
9.6. Timely Maintenance

Recommended documentation includes:

- [ ] **System and Device Management Policy**
- [ ] **System and Device Management Procedure**

- [ ] Control Evidence Document for each System and Device Management defined control
- [ ] List of approved maintenance tools
- [ ] List of approved maintenance personnel

10. MEDIA PROTECTION

Topics addressed by documentation for this control family should include:

10.1. Policy and Procedure
10.2. Media Access
10.3. Media Marking
10.4. Media Storage
10.5. Media Transport
10.6. Media Sanitization
10.7. Media Use

Recommended documentation includes:

- [ ] **Media Protection Policy**
- [ ] **Media Protection Procedure**
- [ ] Control Evidence Document for each Media Protection defined control
- [ ] Media inventory
- [ ] Certificates of destruction for destroyed media
- [ ] Sanitization records for re-used media

11. PHYSICAL SECURITY

Topics addressed by documentation for this control family should include:

11.1. Policy and Procedure
11.2. Physical Access Authorizations
11.3. Physical Access Controls

11.4. Access Control for Transmission Lines
11.5. Access Control for Output Devices
11.6. Monitoring Physical Access
11.7. Visitor Access Records
11.8. Power Equipment and Cabling
11.9. Emergency Shutoff
11.10. Uninterruptible Power Supply
11.11. Emergency Lighting
11.12. Fire Protection
11.13. Environmental Controls
11.14. Water Damage Protection
11.15. Delivery and Removal
11.16. Alternate Work Site(s)

Recommended documentation includes:

- [ ] **Physical Security Policy**
- [ ] **Physical Security Procedure**
- [ ] Control Evidence Document for each Physical Security defined control
- [ ] List of physical access authorizations
- [ ] Records of physical access authorization reviews
- [ ] Inventory of physical access devices
- [ ] Records of physical access device inventory reviews
- [ ] Visitor access logs
- [ ] Records of visitor access log reviews
- [ ] Uninterruptible power supply testing records
- [ ] Name and location of alternate work site(s)

12. SYSTEM SECURITY PLANNING

Topics addressed by documentation for this control family should include:

12.1. Policy and Procedure
12.2. System Security Plans
12.3. Rules of Behavior
12.4. Security and Privacy Architectures
12.5. Centralized Management
12.6. Baseline Control Selection
12.7. Baseline Control Tailoring

Recommended documentation includes:

- [ ] **System Security Planning Policy**
- [ ] **System Security Planning Procedure**
- [ ] Control Evidence Document for each System Security Planning defined control
- [ ] System Security Plan
- [ ] Rules of Behavior
- [ ] Security and privacy architecture diagrams and associated documentation
- [ ] Baseline control selection
- [ ] Baseline control tailoring

13. SECURITY PROGRAM MANAGEMENT

Topics addressed by documentation for this control family should include:

13.1. Security Program Plan
13.2. Security Program Leadership Role
13.3. Security program Resources
13.4. Plans of Action and Milestones
13.5. Information System Inventories
13.6. Measures of Performance

13.7. Enterprise Architecture
13.8. Critical Infrastructure Plan
13.9. Risk Management Strategy
13.10. Authorization Process
13.11. Mission and Business Process Definition
13.12. Insider Threat Program
13.13. Security and Privacy Workforce
13.14. Testing Training, and Monitoring
13.15. Security and Privacy Groups and Associations
13.16. Threat Awareness Program
13.17. Protecting Controlled Unclassified Information on External Systems
13.18. Privacy Program Plan
13.19. Privacy Program Leadership Role
13.20. Dissemination of Privacy Program Information
13.21. Accounting of Disclosures
13.22. PII Quality Management
13.23. Data Governance Body
13.24. Data Integrity Board
13.25. Minimization of PII Used in Testing, Training, and Research
13.26. Compliance Management Process
13.27. Privacy Reporting
13.28. Risk Framing
13.29. Risk Management Program Leadership Roles
13.30. Supply Chain Risk Management Strategy
13.31. Continuous Monitoring Strategy
13.32. Purposing

Recommended documentation includes:

- [ ] **Security Program Management Policy**
- [ ] **Security Program Management Procedure**
- [ ] Control Evidence Document for each Security Program Management defined control
- [ ] Information system inventories
- [ ] Inventory of systems that process or store PII

- [ ] Measures of Security Program performance
- [ ] Enterprise architecture diagrams
- [ ] Critical infrastructure plan
- [ ] Risk management strategy
- [ ] Insider threat program plan
- [ ] List of security groups and associations with which the organization interacts
- [ ] Threat awareness program documentation
- [ ] Privacy program plan
- [ ] Accounting of disclosures, if applicable
- [ ] Complaint management records, if applicable
- [ ] Supply chain risk management strategy
- [ ] List of critical suppliers
- [ ] Continuous monitoring strategy

14. PERSONNEL SECURITY

Topics addressed by documentation for this control family should include:

14.1. Policy and Procedure
14.2. Position Risk Designations
14.3. Personnel Screening
14.4. Personnel Terminations
14.5. Personnel Transfers
14.6. Access Agreements
14.7. Third-Party Personnel Security
14.8. Personnel Sanctions
14.9. Position Descriptions

Recommended documentation includes:

- [ ] **Personnel Security Policy**
- [ ] **Personnel Security Procedure**
- [ ] Control Evidence Document for each Personnel Security defined control
- [ ] Position risk designations
- [ ] Personnel screening criteria
- [ ] Personnel termination process and checklist
- [ ] Personnel transfer process and checklist
- [ ] Access agreements (templates and executed)
- [ ] Personnel sanction process
- [ ] Position descriptions

15. PII PROCESSING AND TRANSPARENCY

Topics addressed by documentation for this control family should include:

15.1. Policy and Procedures
15.2. Authority to Process PII
15.3. PII Processing Purposes
15.4. Consent
15.5. Privacy notices
15.6. System of Record Notices (SORNs)
15.7. Specific PII Categories
15.8. Computer Matching Agreements

Recommended documentation includes:

- [ ] **PII Processing and Transparency Policy**
- [ ] **PII Processing and Transparency Procedure**

- [ ] Control Evidence Document for each PII Processing and Transparency defined control
- [ ] Documented authority to process PII
- [ ] Defined PII processing purposes
- [ ] Privacy notices
- [ ] Privacy Act Statements
- [ ] System of Records Notices (SORNs)
- [ ] List of specific PII categories
- [ ] Computer matching agreements

16. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

16.1. Policy and Procedure
16.2. Security Categorizations
16.3. Performing Risk Assessments
16.4. Vulnerability Monitoring and Scanning
16.5. Risk Response
16.6. Privacy Impact Assessments
16.7. Criticality Analysis

Recommended documentation includes:

- [ ] **Risk Management Policy**
- [ ] **Risk Management Procedure**
- [ ] Control Evidence Document for each Risk Management defined control
- [ ] Risk assessment questionnaire
- [ ] Risk assessment results

- [ ] System-generated vulnerability monitoring and scanning reports
- [ ] Records of updating vulnerabilities for which to scan
- [ ] Records of risk response activities
- [ ] Vulnerability management metrics
- [ ] Privacy impact assessments
- [ ] Criticality analysis records

17. SYSTEM AND SERVICE ACQUISITION

Topics addressed by documentation for this control family should include:

17.1. Policy and Procedure
17.2. Allocation of Resources
17.3. System Development Life Cycle (SDLC)
17.4. Acquisition Process
17.5. System Documentation
17.6. Security and Privacy Engineering Principles
17.7. External System Services
17.8. Configuration Management for Developers
17.9. Developer Testing and Evaluation
17.10. Develop Processes, Standards, and Tools
17.11. Unsupported System Components

Recommended documentation includes:

- [ ] **System and Service Acquisition Policy**
- [ ] **System and Service Acquisition Procedure**
- [ ] Control Evidence Document for each System and Service Acquisition defined control
- [ ] System development life cycle (SDLC) program documentation
- [ ] Security and privacy engineering principles

☐ List of functions, ports, protocols, and services for external system services

☐ List of unsupported system components, if applicable

18. SYSTEM AND COMMUNICATIONS SECURITY

Topics addressed by documentation for this control family should include:

18.1. Policy and Procedure
18.2. Separation of System and User Functionality
18.3. Information in Shared System Resources
18.4. Denial of Service Protection
18.5. Boundary Protection
18.6. Transmission Confidentiality and Integrity
18.7. Network Disconnects
18.8. Cryptographic Key Management
18.9. Cryptographic Protection
18.10. Collaborative Computing Devices and Applications
18.11. Public Key Infrastructure (PKI) Certificates
18.12. Mobile Code
18.13. Secure Name and Address Resolution Service (Authoritative Source)
18.14. Secure Name and Address Resolution Service (Recursive or Caching Resolver)
18.15. Architecture and Provisioning for Name and Address Resolution Service
18.16. Session Authenticity
18.17. Protecting Information at Rest
18.18. Process Isolation

Recommended documentation includes:

☐ **System and Communications Security Policy**

☐ **System and Communications Security Procedure**

☐ Control Evidence Document for each System and Communications Security defined control

☐ Cryptographic key management process documentation

- [ ] Cryptographic key inventory
- [ ] List of approved mobile code
- [ ] Encryption configuration settings for data at rest
- [ ] Encryption configuration settings for data in transit

19. SYSTEM AND INFORMATION INTEGRITY

Topics addressed by documentation for this control family should include:

19.1. Policy and Procedure
19.2. Flaw Remediation
19.3. Malicious Code Protection
19.4. System Monitoring
19.5. Security Alerts, Advisories, and Directives
19.6. Software, Firmware, and Information integrity
19.7. Spam Protection
19.8. Information Input Validation
19.9. Error Handling
19.10. Information management and Retention
19.11. Memory Protection
19.12. PII Quality Operations
19.13. De-Identification of PII

Recommended documentation includes:

- [ ] **System and Information Security Policy**
- [ ] **System and Information Security Procedure**
- [ ] Control Evidence Document for each System and Information Security defined control
- [ ] Flaw remediation metrics
- [ ] List of all systems and components

- [ ] System-generated list of systems and components with anti-malware software installed
- [ ] System monitoring results
- [ ] Sampling of system-generated alerts
- [ ] Security alerts, advisories, and directives received by the organization
- [ ] Spam protection configuration documentation
- [ ] Records retention schedule

20. SUPPLY CHAIN RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

20.1. Policy and Procedure
20.2. Supply Chain Risk Management Plan
20.3. Supply Chain Controls and Processes
20.4. Acquisition Strategies, Tools, and Methods
20.5. Supplier Assessments and Reviews
20.6. Notification Agreements
20.7. Inspection of Systems or Components
20.8. Component Authenticity
20.9. Component Disposal

Recommended documentation includes:

- [ ] **Supply Chain Risk Management Policy**
- [ ] **Supply Chain Risk Management Procedure**
- [ ] Control Evidence Document for each Supply Chain Risk Management defined control
- [ ] Supply chain risk management plan
- [ ] Records of supplier assessments and reviews

- [ ] Records of inspection of systems or components
- [ ] Records of component disposal

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.