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 FedRAMP 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.

FedRAMP is comprised of 17 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 Notifications
1.9. Concurrent Session Control
1.10. Device Locks
1.11. Session Terminations
1.12. Permitted Actions without Identification or Authentication
1.13. Remote Access
1.14. Wireless Access
1.15. Access Control for Mobile Devices
1.16. Use of External Information Systems
1.17. Information Sharing
1.18. Publicly Accessible Content

Recommended documentation includes:

- [ ] **Access Control Policy**
- [ ] **Access Control Procedure**
- [ ] Control Evidence Document for each Access Control defined control
- [ ] List of all user accounts
- [ ] List of all personnel
- [ ] List of recently terminated personnel
- [ ] List of recently onboarded personnel
- [ ] List of disabled accounts due to inactivity
- [ ] Role-based access control matrix
- [ ] Data flow diagrams
- [ ] List of privileged accounts
- [ ] Privileged account auditing reports
- [ ] System-generated reports of unsuccessful logon attempts
- [ ] Logon banners or system use notifications
- [ ] List of users with authorized remote access
- [ ] Inventory of access control points
- [ ] Inventory of wireless access points
- [ ] Inventory of mobile devices
- [ ] Encryption configuration settings for mobile devices
- [ ] Inventory of portable storage devices

☐ Records of publicly available content reviews

2. SECURITY AWARENESS TRAINING

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 Policy**

☐ **Security Awareness Training Procedure**

☐ Control Evidence Document for each Security Awareness Training 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. Audit Events
3.3. Content of Audit Records
3.4. Audit Log Storage Capacity
3.5. Response to Audit Processing Failures
3.6. Audit Record Analysis and Reporting
3.7. Audit Reduction and Report Generation
3.8. Time Stamps

3.9. Protection of Audit Log Information
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
- [ ] Records of reviewing and updating the list of event types logged
- [ ] Records of actions taken in response to audit processing failures
- [ ] List of authoritative time sources
- [ ] Audit record retention schedule

4. SECURITY ASSESSMENTS AND MONITORING

Topics addressed by documentation for this control family should include:

4.1. Policy and Procedure
4.2. Security Assessments
4.3. System Interconnections
4.4. Plan of Actions and Milestones
4.5. Security Authorizations
4.6. Continuous Monitoring
4.7. Penetration Testing
4.8. Internal System Connections

Recommended documentation includes:

- [ ] **Security Assessments and Monitoring Policy**
- [ ] **Security Assessments and Monitoring Procedure**

- [ ] Control Evidence Document for each Security Assessments and Monitoring defined control
- [ ] Security assessment reports
- [ ] Network diagrams
- [ ] Plans of Action and Milestones (POAMs)
- [ ] Records of monthly POAM reviews and updates
- [ ] System security authorizations
- [ ] Continuous monitoring plan
- [ ] Independent assessment reports
- [ ] Penetration testing reports

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 Change
5.6. Configuration Settings
5.7. Least Functionality
5.8. Information System Component Inventory
5.9. Configuration Management Plan
5.10. Software Usage Restrictions
5.11. User Installed Software

Recommended documentation includes:

- [ ] **Configuration Management Policy**
- [ ] **Configuration Management Procedure**

- [ ] Control Evidence Document for each Configuration Management defined control
- [ ] Baseline configurations for systems and devices
- [ ] Evidence of baseline configurations reviews and updates
- [ ] System configurations for high-risk areas
- [ ] Configuration change control records
- [ ] Security impact analysis results
- [ ] Information system component inventory
- [ ] Evidence of information system component inventory reviews and updates
- [ ] Configuration Management Plan

6. CONTINGENCY PLANNING

Topics addressed by documentation for this control family should include:

6.1. Policy and Procedure
6.2. Contingency Plans
6.3. Contingency Plan Training
6.4. Contingency Plan Testing
6.5. Alternate Storage Site
6.6. Alternate Processing Site
6.7. Telecommunications Services
6.8. Information System Backups
6.9. Information System Recovery and Reconstitution

Recommended documentation includes:

- [ ] **Contingency Planning Policy**
- [ ] **Contingency Planning Procedure**
- [ ] Control Evidence Document for each Contingency Planning defined control

- [ ] Contingency plans
- [ ] Capacity planning documentation
- [ ] Contingency plan training materials and records
- [ ] Contingency plan test scripts
- [ ] Contingency plan testing reports
- [ ] Names and locations of alternate storage sites
- [ ] Names and locations of alternate processing sites
- [ ] Information system backup schedule
- [ ] Records of regular backup data 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. Authenticator Feedback
7.7. Cryptographic Module Authentication
7.8. Identification and Authentication for External Users

Recommended documentation includes:

- [ ] **Identification and Authentication Policy**
- [ ] **Identification and Authentication Procedure**
- [ ] Control Evidence Document for each Identification and Authentication defined control

- [ ] Inventory of identification and authentication devices

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
8.9. Information Spillage Response

Recommended documentation includes:

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

9. SYSTEM AND DEVICE MAINTENANCE

Topics addressed by documentation for this control family should include:

9.1. Policy and Procedure
9.2. Controlled Maintenance

9.3. Maintenance Tools
9.4. Non-Local Maintenance
9.5. Maintenance Personnel
9.6. Timely Maintenance

Recommended documentation includes:

- [ ] **System and Device Maintenance Policy**
- [ ] **System and Device Maintenance Procedure**
- [ ] Control Evidence Document for each System and Device Maintenance defined control
- [ ] List of approved maintenance tools
- [ ] List of approved maintenance personnel
- [ ] System and device maintenance records

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 Authorization
11.3. Physical Access Control
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. Emergency Power
11.11. Emergency Lighting
11.12. Fire Protection
11.13. Temperature and Humidity Controls
11.14. Water Damage Protection
11.15. Delivery and Removal
11.16. Alternate Work Sites

Recommended documentation includes:

- [ ] **Physical Security Policy**
- [ ] **Physical Security Procedure**
- [ ] Control Evidence Document for each Physical Security defined control
- [ ] List of physical access authorizations
- [ ] Inventory of physical access devices
- [ ] Physical access logs

- [ ] Records of physical access log reviews
- [ ] Visitor logs
- [ ] Records of visitor log reviews
- [ ] Names and locations of alternate work sites

12. SECURITY PROGRAM 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 Architectures

Recommended documentation includes:

- [ ] **Security Program Planning Policy**
- [ ] **Security Program Planning Procedure**
- [ ] Control Evidence Document for each Security Program Planning defined control
- [ ] System Security Plan
- [ ] Rules of Behavior
- [ ] Security Architectures

13. PERSONNEL SECURITY

Topics addressed by documentation for this control family should include:

13.1. Policy and Procedure
13.2. Position Risk Designations
13.3. Personnel Screening
13.4. Personnel Terminations

13.5. Personnel Transfers
13.6. Access Agreements
13.7. Third-Party Personnel Security
13.8. Personnel Sanctions

Recommended documentation includes:

- [ ] **Personnel Security Policy**
- [ ] **Personnel Security Procedure**
- [ ] Control Evidence Document for each Personnel Security defined control
- [ ] Position risk designations
- [ ] Personnel screening criteria and results
- [ ] Personnel termination process and records
- [ ] Personnel transfer process and records
- [ ] Personnel access agreements (template and executed)
- [ ] Third-party personnel security requirements
- [ ] Personnel sanction examples, if applicable

14. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

14.1. Policy and Procedure
14.2. Security Categorization
14.3. Performing Risk Assessments
14.4. Vulnerability Management

Recommended documentation includes:

- [ ] **Risk Management Policy**
- [ ] **Risk Management Procedure**

- [ ] Control Evidence Document for each Risk Management defined control
- [ ] Security categorization for critical systems
- [ ] Risk assessments
- [ ] Risk assessment results
- [ ] Vulnerability scanning schedule
- [ ] Vulnerability remediation schedule
- [ ] Vulnerability management metrics
- [ ] Vulnerability scanning reports

15. SYSTEM AND SERVICE ACQUISITION

Topics addressed by documentation for this control family should include:

15.1. Policy and Procedure
15.2. Allocation of Resources
15.3. System Development Life Cycle
15.4. Acquisition Process
15.5. Information System Documentation
15.6. Security Engineering Principles
15.7. External Information System Services
15.8. Developer Configuration Management
15.9. Developer Security testing and Evaluation

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) documentation

- [ ] Acquisition process documentation
- [ ] List of functions, port, protocols, services for new acquisitions
- [ ] List of approved PIV products, if applicable
- [ ] Security engineering principles
- [ ] List of external information system services
- [ ] Risk assessment results for systems or services prior to acquisition
- [ ] List of processing, storage, and service locations
- [ ] Developer configuration management plan
- [ ] Software and firmware integrity verification results
- [ ] Developer security testing and evaluation results

16. SYSTEM AND COMMUNICATIONS PROTECTION

Topics addressed by documentation for this control family should include:

16.1. Policy and Procedure
16.2. Separation of System and User Functionality
16.3. Information in Shared Resources
16.4. Denial of Service Protection
16.5. Resource Availability
16.6. Boundary Protection
16.7. Transmission Confidentiality and Integrity
16.8. Network Disconnect
16.9. Cryptographic Key Management
16.10. Cryptographic Protection
16.11. Collaborative Computing Devices
16.12. Public Key Infrastructure Certificates
16.13. Mobile Code
16.14. Voice over Internet Protocol
16.15. Authoritative Source Name and Address Resolution Service

16.16. Recursive or Caching Resolver Name and Address Resolution Service
16.17. Name and Address Resolution Service Architecture and Provisioning
16.18. Session Authenticity
16.19. Protection of Information at Rest
16.20. Process Isolation

Recommended documentation includes:

- [ ] **System and Communication Protection Policy**
- [ ] **System and Communication Protection Procedure**
- [ ] Control Evidence Document for each System and Communication Protection defined control
- [ ] Cryptographic key management process documentation

17. SYSTEM AND INFORMATION INTEGRITY

Topics addressed by documentation for this control family should include:

17.1. Policy and Procedure
17.2. Flaw Remediation
17.3. Malicious Code Protection
17.4. Information System Monitoring
17.5. Security Alerts, Advisories, and Directives
17.6. Security Function Validation
17.7. Software, Firmware, and Information Integrity
17.8. Spam Protection
17.9. Information Input Validation
17.10. Error Handling
17.11. Information Handling and Retention
17.12. System memory Protection

Recommended documentation includes:

- [ ] **System and Information Integrity Policy**
- [ ] **System and Information Integrity Procedure**

- [ ] Control Evidence Document for each System and Information Integrity defined control
- [ ] Flaw remediation metrics
- [ ] List of information system components
- [ ] System-generated report of information system components with anti-malware software installed
- [ ] Information system monitoring results
- [ ] Security alerts, advisories, and directives received by the organization
- [ ] Spam protection configuration documentation

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.