Documentation Checklist for NIST Cybersecurity Framework (CSF)

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 CSF 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.

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. ASSET MANAGEMENT

Topics addressed by documentation for this control family should include:

1.1. Hardware Asset Management
1.2. Software Asset Management
1.3. Data Flow Diagrams and Mapping
1.4. Inventory of External Information Systems
1.5. Resource Classification and Prioritization
1.6. Roles and Responsibilities

Recommended documentation includes:

- [ ] **Asset Management Policy**
- [ ] **Asset Management Procedure**
- [ ] Control Evidence Document for each Asset Management defined control
- [ ] Hardware asset inventory
- [ ] Software asset inventory
- [ ] Data flow diagrams
- [ ] External system inventory

☐ Roles and responsibilities matrix

2. BUSINESS ENVIRONMENT

Topics addressed by documentation for this control family should include:

2.1. Supply Chain Role
2.2. Critical Infrastructure Role
2.3. Organizational Mission, Objectives, and Activities
2.4. Critical Functions and Dependencies
2.5. Business Resiliency Requirements

Recommended documentation includes:

☐ **Business Environment Policy**

☐ **Business Environment Procedure**

☐ Control Evidence Document for each Business Environment defined control

☐ Business Impact Analysis results

3. SECURITY PROGRAM GOVERNANCE

Topics addressed by documentation for this control family should include:

3.1. Communicating Security Program Policies
3.2. Security Program Roles and Responsibilities
3.3. Legal and Regulatory Requirements
3.4. Governance and Risk Management Processes

Recommended documentation includes:

☐ **Security Program Governance Policy**

☐ **Security Program Governance Procedure**

☐ Control Evidence Document for each Security Program Governance defined control

☐ Evidence of communicating policies to appropriate personnel

- [ ] Security Program roles and responsibilities matrix
- [ ] List of applicable legal and regulatory compliance

4. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

- 4.1. Risk Management Strategy
  - 4.1.1. Risk Management Processes
  - 4.1.2. Risk Tolerance
  - 4.1.3. Risk Analysis
- 4.2. Risk Assessments
  - 4.2.1. Vulnerability Management
  - 4.2.2. Threat Intelligence
  - 4.2.3. Potential Business Impacts
  - 4.2.4. Risk Determination
  - 4.2.5. Responding to Risks
- 4.3. Supply Chain Risk Management
  - 4.3.1. Supply Chain Risk Management Processes
  - 4.3.2. Prioritizing Third-Party Providers
  - 4.3.3. Third-Party Provider Contracts
  - 4.3.4. Third-Party Provider Due Diligence
  - 4.3.5. Planning and Testing with Providers

Recommended documentation includes:

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

- [ ] List of risk-ranked third-party providers
- [ ] Security controls for third-party providers
- [ ] Third-party provider due diligence results
- [ ] Results of plan testing with critical third parties, if applicable

5. ACCESS CONTROL

Topics addressed by documentation for this control family should include:

5.1. Identity Management
5.2. Physical Access Management
5.3. Logical Access Management
5.4. Remote Access Management
5.5. Principle of Least Privilege
5.6. Network Integrity
5.7. Unique User Identification
5.8. User and Device Authentication

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 service accounts
- [ ] List of all personnel
- [ ] List of assign physical access permissions for personnel
- [ ] Evidence of regular logical access reviews
- [ ] Evidence of regular physical access review

- [ ] Evidence of regular logical and physical access log reviews
- [ ] List of recently terminated personnel
- [ ] List of recently onboarded personnel

6. SECURITY AWARENESS TRAINING

Topics addressed by documentation for this control family should include:

6.1. All-Personnel Security Awareness Training
6.2. Role-Based Security Awareness Training
6.3. Third-Party Security Awareness Training
6.4. Executive Leadership Security Awareness Training
6.5. Security Personnel Security Awareness Training

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 records/reports

7. DATA SECURITY

Topics addressed by documentation for this control family should include:

7.1. Protecting Data at Rest
7.2. Protecting Data in Transit
7.3. Information Asset Lifecycle Management
7.4. Capacity Monitoring and Management
7.5. Data Leakage Prevention

7.6. Software, Firmware, and Information Integrity
7.7. Separation of Production and Non-Production Environments
7.8. Hardware Integrity

Recommended documentation includes:

- [ ] **Data Security Policy**
- [ ] **Data Security Procedure**
- [ ] Control Evidence Document for each Data Security defined control
- [ ] Encryption configuration settings for data at rest
- [ ] Encryption configuration settings for data in transit
- [ ] Capacity monitoring reports/records
- [ ] Configuration settings and associated documentation for data leakage prevention solutions
- [ ] Evidence of separation for production and non-production systems

8. INFORMATION ASSET PROTECTION

Topics addressed by documentation for this control family should include:

8.1. Security Baseline Configurations
8.2. System Development Life Cycle (SDLC)
8.3. Change Control Management
8.4. Information Backups
8.5. Physical Operating Environment of Information Assets
8.6. Data Destruction
8.7. Continuous Improvement of Information Asset Protection
8.8. Effectiveness of Protection Technologies
8.9. Incident Response and Business Continuity Plans
8.10. Incident Response and Business Continuity Plan Testing
8.11. Security Program Controls for Human Resources (HR) Functions
8.12. Vulnerability Management Plan

Recommended documentation includes:

- [ ] **Information Asset Protection Policy**
- [ ] **Information Asset Protection Procedure**
- [ ] Control Evidence Document for each Information Asset Protection defined control
- [ ] System and device baseline configuration settings
- [ ] SDLC process documentation
- [ ] Change control records
- [ ] Data and configuration backup schedule
- [ ] Evidence of backup data recovery testing
- [ ] Certificates of destruction for destroyed information assets
- [ ] Reports from security monitoring tools
- [ ] Incident Response Plan
- [ ] Business Continuity Plan(s)
- [ ] HR security roles and responsibilities
- [ ] Vulnerability Management Plan
- [ ] Vulnerability management metrics

9. SYSTEM MAINTENANCE

Topics addressed by documentation for this control family should include:

9.1. Information System Maintenance
9.2. Remote Maintenance

Recommended documentation includes:

- [ ] **System Maintenance Policy**
- [ ] **System Maintenance Procedure**
- [ ] Control Evidence Document for each System Maintenance defined control
- [ ] System maintenance records

10. PROTECTIVE TECHNOLOGY

Topics addressed by documentation for this control family should include:

10.1. Audit Logging and Review
10.2. Removable Media Protection
10.3. Least Functionality of Systems
10.4. Network Protection
10.5. Support of Resiliency Requirements

Recommended documentation includes:

- [ ] **Protective Technology Policy**
- [ ] **Protective Technology Procedure**
- [ ] Control Evidence Document for each Protective Technology defined control
- [ ] Evidence of audit log reviews
- [ ] System configuration documentation

11. LOGGING AND MONITORING

Topics addressed by documentation for this control family should include:

11.1. Anomalies and Events
  11.1.1. Baseline of Network Operations
  11.1.2. Analysis of Detected Events
  11.1.3. Event Collection and Correlation
  11.1.4. Determination of Impact of Events
  11.1.5. Incident Thresholds

11.2. Continuous Monitoring
- 11.2.1. Monitoring Network Activity
- 11.2.2. Monitoring the Physical Environment
- 11.2.3. Monitoring Personnel Actions
- 11.2.4. Malicious Code Protection
- 11.2.5. Mobile Code Protection
- 11.2.6. Monitoring External Service Providers
- 11.2.7. Unauthorized Personnel, Connections, Devices, and Software
- 11.2.8. Vulnerability Scanning

Recommended documentation includes:

- [ ] **Logging and Monitoring Policy**
- [ ] **Logging and Monitoring Procedure**
- [ ] Control Evidence Document for each Logging and Monitoring defined control
- [ ] Network activity baseline measures
- [ ] Evidence of detected event analysis
- [ ] Defined incident thresholds
- [ ] Evidence of logical, physical, and personnel activity monitoring
- [ ] List of all information systems
- [ ] System-generated report listing information systems with anti-malware software installed
- [ ] Third-party provider performance reports
- [ ] Vulnerability scanning and remediation results

12. EVENT DETECTION

Topics addressed by documentation for this control family should include:

12.1. Detection Roles and Responsibilities

12.2. Detection Requirements
12.3. Testing Detection Processes
12.4. Communicating Detection Results
12.5. Continuous Improvement of Detection Processes

Recommended documentation includes:

- [ ] **Event Detection Policy**
- [ ] **Event Detection Procedure**
- [ ] Control Evidence Document for each Event Detection defined control
- [ ] Event management roles and responsibilities matrix
- [ ] Detection testing results

13. INCIDENT MANAGEMENT

Topics addressed by documentation for this control family should include:

13.1. Incident Response Plan
13.2. Incident Response Communications
  13.2.1. Roles, Responsibilities, and Order of Communications
  13.2.2. Incident Reporting
  13.2.3. Sharing Incident Information Internally
  13.2.4. Incident Response Coordination
  13.2.5. Sharing Incident Information Externally
13.3. Incident Analysis
  13.3.1. Event Investigation
  13.3.2. Impact Determination
  13.3.3. Incident Forensics
  13.3.4. Incident Categorization
  13.3.5. Security Alerts and Advisories
13.4. Mitigation
  13.4.1. Incident Containment
  13.4.2. Incident Mitigation
  13.4.3. Vulnerability Mitigation
13.5. Continuous Improvement of Incident Response

13.5.1. Lessons Learned
13.5.2. Response Strategy Updates

Recommended documentation includes:

- ☐ **Incident Management Policy**
- ☐ **Incident Management Procedure**
- ☐ Control Evidence Document for each Incident Management defined control
- ☐ Incident Response Plan
- ☐ Incident reports
- ☐ Security alerts and advisories received from external sources
- ☐ Lessons learned meeting agenda and minutes

14. CONTINGENCY PLANNING

Topics addressed by documentation for this control family should include:

14.1. Recovery Planning
14.2. Recovery Improvements
14.2.1. Improving Recovery Plans
14.2.2. Improving Recovery Strategies
14.3. Recovery Communications
14.3.1. Public Relations
14.3.2. Organizational Reputation
14.3.3. Activity Communications

Recommended documentation includes:

- ☐ **Contingency Planning Policy**
- ☐ **Contingency Planning Procedure**
- ☐ Control Evidence Document for each Contingency Planning defined control
- ☐ Recovery plans

- [ ] Lessons learned meeting agenda and minutes
- [ ] Evidence of recovery plan reviews and updates

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.