Documentation Checklist for Cyber Resilience Review (CRR)

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 Cyber Resilience Review (CRR) 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.

CRR is comprised of 10 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. ASSET MANAGEMENT

Topics addressed by documentation for this control family should include:

1.1. Support for Asset Management
1.2. Identifying Core Services
1.3. Prioritizing Core Services
1.4. Common Definition of Assets
1.5. Responsibility for Identifying Assets
1.6. Personnel Assets
1.7. Information Assets
1.8. Technology Assets
1.9. Facility Assets
1.10. Asset Inventory
1.11. Relationships between Assets and Critical Services
1.12. Dependencies between Assets
1.13. Asset Inventory Updates
1.14. Change Criteria
1.15. Change Schedule
1.16. Managing Changes to Assets and Inventories
1.17. Updating the Asset Inventory
1.18. Process Improvement

Recommended documentation includes:

- ☐ **Asset Management Policy**
- ☐ **Asset Management Procedure**
- ☐ Control Evidence Documents for each Asset Management defined control
- ☐ Prioritized list of core services
- ☐ Asset inventory that includes IT assets, data assets, personnel assets, and facility assets

2. SECURITY CONTROLS MANAGEMENT

Topics addressed by documentation for this control family should include:

2.1. Support for Security Control Management
2.2. Establishing Control Objectives
2.3. Identifying Controls
2.4. Analyzing Controls
2.5. Assessing Controls
2.6. Implementing Controls
2.7. Security Requirements Traceability Matrix
2.8. Analyzing Controls against Control Objectives
2.9. Identifying Control Gaps
2.10. Creating New and Updating Existing Controls
2.11. Linking Controls to the Risk Management Process
2.12. Security Requirements Traceability Matrix Updates
2.13. Control Deployment
2.14. Process for Control Assessments
2.15. Scheduling the Assessment of Controls
2.16. Control Assessment Scope
2.17. Performing Control Assessments
2.18. Improving Controls
2.19. Updating Control Objectives and Controls

Recommended documentation includes:

- ☐ **Security Controls Management Policy**

- [ ] **Security Controls Management Procedure**
- [ ] Control Evidence Documents for each Security Controls Management defined control
- [ ] Complete list of control objectives
- [ ] Security requirements traceability matrix
- [ ] Control assessment results

3. CONFIGURATION AND CHANGE MANAGEMENT

Topics addressed by documentation for this control family should include:

3.1. Support for Configuration and Change Management
3.2. Budget for Configuration and Change Management
3.3. Roles and Responsibilities
3.4. Existing Documentation
3.5. Critical Services Requiring Change and Configuration Management
3.6. Establishing a Configuration Change Review Board
3.7. Change Request Process
3.8. Communicating Changes
3.9. Configuration and Change Management Tracking
3.10. Implementing and Monitoring Configurations
3.11. Capacity Management Planning
3.12. Mapping Critical Services to Stakeholders
3.13. Identifying Critical Service Assets
3.14. Configuration Items Requiring Change and Configuration Management
3.15. Configuration Baselines for Configuration Items
3.16. Evaluating Change Requests and Approvals
3.17. Testing Changes
3.18. Deploying Changes
3.19. Success or Failure of Changes
3.20. Roll Back of Unsuccessful Changes
3.21. Change Completion
3.22. Changes to Configuration Baselines
3.23. Monitoring Changes to Configurations

3.24. Undocumented Information Systems or Components
3.25. Disparities between Approved and Implemented Baselines
3.26. Monitoring for Unauthorized Changes
3.27. Comparing Audits and Configuration Control Records
3.28. Remediation Actions

Recommended documentation includes:

- [ ] **Configuration and Change Management Policy**
- [ ] **Configuration and Change Management Procedure**
- [ ] Control Evidence Documents for each Configuration and Change Management defined control
- [ ] Roles and responsibilities matrix
- [ ] Configuration management plan
- [ ] Change management plan
- [ ] Capacity management plan
- [ ] List of configuration items that require change and configuration management
- [ ] Configuration baselines for configuration items

4. VULNERABILITY MANAGEMENT

Topics addressed by documentation for this control family should include:

4.1. Scope of Vulnerability Management
4.2. Approved Vulnerability Assessment Methods
4.3. Vulnerability Assessment Resources
4.4. Vulnerability Management Plan
4.5. Measures of Effectiveness
4.6. Training Requirements
4.7. Tool Selection
4.8. Sources of Vulnerability Information

4.9. Roles and Responsibilities
4.10. Engaging Stakeholders
4.11. Vulnerability Management Plan Revisions
4.12. Vulnerability Management Training
4.13. Performing Vulnerability Assessments
4.14. Recording Discovered Vulnerabilities
4.15. Vulnerability Categories and Prioritization
4.16. Managing Exposure to Vulnerabilities
4.17. Effectiveness of Vulnerability Management
4.18. Root Cause Analysis
4.19. Continuous Improvement

Recommended documentation includes:

- [ ] **Vulnerability Management Policy**
- [ ] **Vulnerability Management Procedure**
- [ ] Control Evidence Documents for each Vulnerability Management defined control
- [ ] List of vulnerability assessment resources
- [ ] Roles and responsibilities matrix
- [ ] Vulnerability management plan
- [ ] Vulnerability management training materials and records
- [ ] Vulnerability management metrics

5. INCIDENT MANAGEMENT

Topics addressed by documentation for this control family should include:

5.1. Support for Incident Management Planning
5.2. Event Detection Process
5.3. Triage and Analysis
5.4. Incident Declaration
5.5. Incident Response and Recovery

5.6. Incident Communications
5.7. Post-Incident Analysis and Improvement
5.8. Roles and Responsibilities for Incident Management
5.9. Testing the Incident Management Plan

Recommended documentation includes:

- [ ] **Incident Management Policy**
- [ ] **Incident Management Procedure**
- [ ] **Incident Management Plan**
- [ ] Control Evidence Documents for each Incident Management defined control
- [ ] Roles and responsibilities matrix
- [ ] Incident management test scripts
- [ ] Incident management testing reports
- [ ] Incident management training materials and records

6. BUSINESS CONTINUITY

Topics addressed by documentation for this control family should include:

6.1. Support for Business Continuity Planning
6.2. Program Design and Supporting Documentation
6.3. Business Impact Analysis
6.4. Business Continuity Training and Awareness
6.5. Linking Incident Response and Recovery Processes
6.6. Identifying Business Continuity Plans to be Developed
6.7. Developing Business Continuity Plans
6.8. Assigning Personnel
6.9. Business Continuity Plan Repository
6.10. Plan Activation and Execution
6.11. Business Continuity Plan Reviews
6.12. Testing Strategy, Process, and Schedule
6.13. Business Continuity Plan Testing

6.14. Evaluating Test Results
6.15. After Action Reviews
6.16. Business Continuity Training
6.17. Reviewing Business Continuity Effectiveness
6.18. Conditions for Revising Business Continuity Plans

Recommended documentation includes:

- [ ] **Business Continuity Policy**
- [ ] **Business Continuity Procedure**
- [ ] Control Evidence Documents for each Business Continuity defined control
- [ ] Roles and responsibilities matrix
- [ ] Business impact analysis results
- [ ] Business continuity training materials and records
- [ ] Business continuity plans
- [ ] Evidence of business continuity plan reviews
- [ ] Business continuity plan testing strategy, process, and schedule
- [ ] Business continuity plan test scripts
- [ ] Business continuity plan testing results

7. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

7.1. Support for Risk Management Planning
7.2. Risk Management Strategy
7.3. Managing Operational Risk Documentation
7.4. Preparing to Implement the Risk Management Strategy
7.5. Risk Communication Process
7.6. Assigning Responsibility for Implementing the Risk Management Plan

7.7. Risk Management Plan Training
7.8. Risk identification Process
7.9. Risk Analysis Process
7.10. Risk Disposition Process
7.11. Risk Mitigation
7.12. Risk Monitoring
7.13. Implementing Risk Mitigation and Monitoring
7.14. Communicating Risk Mitigations
7.15. Ensuring Risk management Objectives are Met
7.16. Risk Management Plan Updates and Reporting
7.17. Risk Management Plan Improvements

Recommended documentation includes:

- [ ] **Risk Management Policy**
- [ ] **Risk Management Procedure**
- [ ] Control Evidence Documents for each Risk Management defined control
- [ ] Risk management strategy
- [ ] Risk management plan
- [ ] Roles and responsibilities matrix
- [ ] Risk management plan training materials and records
- [ ] Risk assessment
- [ ] Risk assessment results

8. EXTERNAL DEPENDENCIES MANAGEMENT

Topics addressed by documentation for this control family should include:

8.1. External Dependencies Support and Strategy
8.2. Relationship Formation Planning
8.3. Identifying and Prioritizing External Dependencies
8.4. Relationship Management

8.5. Information Management
8.6. External Dependencies Management Plan
8.7. Responsibilities for Implementing the Plan
8.8. Dependencies on Public Services and Infrastructure Service Providers
8.9. Establishing and Maintaining Relationships with External Entities
8.10. Prioritizing Dependencies
8.11. Monitoring Performance
8.12. Managing Ongoing Relationships

Recommended documentation includes:

- [ ] **External Dependencies Management Policy**
- [ ] **External Dependencies Management Procedure**
- [ ] Control Evidence Documents for each External Dependencies Management defined control
- [ ] External dependencies management strategy
- [ ] Roles and responsibilities matrix
- [ ] List of external dependencies
- [ ] External dependencies management plan

9. SECURITY AWARENESS TRAINING

Topics addressed by documentation for this control family should include:

9.1. Support for Training and Awareness
9.2. Security Awareness Program Strategy
9.3. Building a Training Capability
9.4. Building an Awareness Capability
9.5. Identifying Training Needs
9.6. Identifying Awareness Needs
9.7. Training and Awareness Needs Analysis
9.8. Developing Training and Awareness Materials
9.9. Procuring Third Party Provider Services

9.10. Conducting Training and Awareness Activities
9.11. Training and Awareness Program Evaluation
9.12. Training and Awareness Program Improvements
9.13. Training and Awareness Program Updates

Recommended documentation includes:

- [ ] **Security Awareness Training Policy**
- [ ] **Security Awareness Training Procedure**
- [ ] Control Evidence Documents for each Security Awareness Training defined control
- [ ] Security awareness training program strategy
- [ ] Roles and responsibilities matrix
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training records

10. SITUATIONAL AWARENESS

Topics addressed by documentation for this control family should include:

10.1. Support for Situational Awareness
10.2. Situational Awareness Program Strategy
10.3. Approach to Collecting and Analyzing Situational Awareness Data
10.4. Communicating Situational Awareness Data
10.5. Situational Awareness Plan
10.6. Situational Awareness Data Collections and Analysis Requirements
10.7. Threat Monitoring
10.8. Situational Awareness Communications
10.9. Communication Standards and Guidelines
10.10. Communicating Situational Awareness Information
10.11. Situational Awareness Program Effectiveness
10.12. Situational Awareness Program Improvements

Recommended documentation includes:

- [ ] **Situational Awareness Policy**
- [ ] **Situational Awareness Procedure**
- [ ] Control Evidence Documents for each Situational Awareness defined control
- [ ] Situational awareness program strategy
- [ ] Roles and responsibilities matrix
- [ ] Situational awareness plan
- [ ] Situational awareness communications (sampling)
- [ ] Communication standards and guidelines

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.