Documentation Checklist for FFIEC's Cybersecurity Assessment Tool (CAT)

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 the FFIEC Cybersecurity Assessment Tool (CAT) 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.

The CAT is comprised of 15 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. GOVERNANCE

Topics addressed by documentation for this control family should include:

1.1. Oversight
1.2. Strategy and Policies
1.3. IT Asset Management

Recommended documentation includes:

- [ ] **Governance Policy**
- [ ] **Governance Procedure**
- [ ] Control Evidence Document for each of the defined Governance controls
- [ ] Security Program Plan
- [ ] Security Program Policies
- [ ] IT asset inventory
- [ ] Data inventory
- [ ] Evidence of regular reviews and updates to the IT asset inventory

☐ Evidence of regular reviews and updates to the data inventory

2. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

2.1. Risk Management Program
2.2. Risk Assessments
2.3. Audit

Recommended documentation includes:

☐ **Risk Management Policy**

☐ **Risk Management Procedure**

☐ Control Evidence Document for each of the Risk Management defined controls

☐ Risk assessment

☐ Risk assessment report

3. RESOURCE MANAGEMENT

Topics addressed by documentation for this control family should include:

3.1. Staffing

Recommended documentation includes:

☐ **Resource Management Policy**

☐ **Resource Management Procedure**

☐ Control Evidence Document for each of the Resource Management defined controls

☐ Security Program roles and responsibilities matrix

4. TRAINING AND CULTURE

Topics addressed by documentation for this control family should include:

4.1. Training
4.2. Culture

Recommended documentation includes:

- [ ] **Training and Culture Policy**
- [ ] **Training and Culture Procedure**
- [ ] Control Evidence Document for each of the Training and Culture defined controls
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training records

5. THREAT INTELLIGENCE

Topics addressed by documentation for this control family should include:

5.1. Threat Intelligence and Information Sharing

Recommended documentation includes:

- [ ] **Threat Intelligence Policy**
- [ ] **Threat Intelligence Procedure**
- [ ] Control Evidence Document for each of the Threat Intelligence defined controls
- [ ] Threat intelligence reports

6. MONITORING AND ANALYSIS

Topics addressed by documentation for this control family should include:

6.1. Activity monitoring and Analysis

Recommended documentation includes:

- [ ] **Monitoring and Analysis Policy**
- [ ] **Monitoring and Analysis Procedure**
- [ ] Control Evidence Document for each of the Monitoring and Analysis defined controls
- [ ] Cybersecurity monitoring plan
- [ ] List of events logged by the organization
- [ ] Evidence that the list of events that are logged is reviewed and updated at least annually
- [ ] Evidence of reviewing reports of events and alerts

7. INFORMATION SHARING

Topics addressed by documentation for this control family should include:

7.1. Sharing Threat Information

Recommended documentation includes:

- [ ] **Information Sharing Policy**
- [ ] **Information Sharing Procedure**
- [ ] Control Evidence Document for each of the Information Sharing defined controls
- [ ] Evidence of communicating threat information to appropriate stakeholders

8. PREVENTIVE CONTROLS

Topics addressed by documentation for this control family should include:

8.1. Infrastructure Management
8.2. Access and Data Management
8.3. Device and Endpoint Security
8.4. Secure Coding Practices

Recommended documentation includes:

- [ ] **Preventive Controls Policy**
- [ ] **Preventive Controls Procedure**
- [ ] Control Evidence Document for each of the defined Preventive Controls
- [ ] System and device maintenance records
- [ ] List of security monitoring tools and technologies
- [ ] System-generated report listing assets protected with anti-malware software
- [ ] Secure coding practices
- [ ] Secure coding training materials
- [ ] Secure coding training records

9. DETECTIVE CONTROLS

Topics addressed by documentation for this control family should include:

9.1. Threat and Vulnerability Detection
9.2. Anomalous Activity Detection
9.3. Event Detection

Recommended documentation includes:

- [ ] **Detective Controls Policy**
- [ ] **Detective Controls Procedure**

- [ ] Control Evidence Document for each of the defined Detective Controls
- [ ] Vulnerability management plan
- [ ] Vulnerability scanning schedule
- [ ] Vulnerability scanning metrics
- [ ] Security monitoring reports

10. CORRECTIVE CONTROLS

Topics addressed by documentation for this control family should include:

10.1. Patch Management
10.2. Remediation

Recommended documentation includes:

- [ ] **Corrective Controls Policy**
- [ ] **Corrective Controls Procedure**
- [ ] Control Evidence Document for each of the defined Corrective Controls
- [ ] Vulnerability remediations schedule
- [ ] Vulnerability remediation metrics

11. CONNECTION MANAGEMENT

Topics addressed by documentation for this control family should include:

11.1. Managing External Connections

Recommended documentation includes:

- [ ] **Connection Management Policy**
- [ ] **Connection Management Procedure**

- [ ] Control Evidence Document for each of the Connection Management defined controls
- [ ] List of all external connections

12. RELATIONSHIP MANAGEMENT

Topics addressed by documentation for this control family should include:

12.1. Due Diligence
12.2. Contracts
12.3. Ongoing Monitoring

Recommended documentation includes:

- [ ] **Relationship Management Policy**
- [ ] **Relationship Management Procedure**
- [ ] Control Evidence Document for each of the Relationship Management defined controls
- [ ] Inventory of all third-party providers and suppliers
- [ ] Risk ranking of third-party providers and suppliers
- [ ] Due diligence assessment materials
- [ ] Due diligence results
- [ ] Provider and supplier monitoring plan

13. INCIDENT RESILIENCE PLANNING AND STRATEGY

Topics addressed by documentation for this control family should include:

13.1. Planning
13.2. Testing

Recommended documentation includes:

- [ ] **Incident Resilience Planning and Strategy Policy**
- [ ] **Incident Resilience Planning and Strategy Procedure**
- [ ] **Incident Response Plan**
- [ ] Control Evidence Document for each of the Incident Resilience Planning and Strategy defined controls
- [ ] Incident response test scripts
- [ ] Incident response testing reports

14. INCIDENT DETECTION, RESPONSE, AND MITIGATION

Topics addressed by documentation for this control family should include:

14.1. Detection
14.2. Response and Mitigation

Recommended documentation includes:

- [ ] **Incident Detection, Response, and Mitigation Policy**
- [ ] **Incident Detection, Response, and Mitigation Procedure**
- [ ] Control Evidence Document for each of the Incident Detection, Response, and Mitigation defined controls
- [ ] Incident reports containing mitigation actions

15. INCIDENT ESCALATION AND REPORTING

Topics addressed by documentation for this control family should include:

15.1. Escalation and Reporting Process

Recommended documentation includes:

- [ ] **Incident Escalation and Reporting Policy**

- [ ] **Incident Escalation and Reporting Procedure**
- [ ] Control Evidence Document for each of the Incident Escalation and Reporting defined controls
- [ ] Evidence of communicating security incidents and/or data breaches

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.