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 FFIEC IT Examination Handbooks 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. SECURITY PROGRAM PLANNING

Topics addressed by documentation for this control family should include:

1.1. Security Program Governance
1.2. Management of the Security Program
1.3. Risk Identification
1.4. Risk Measurement
1.5. Risk Mitigation
1.6. Inventory and Classification of Assets
1.7. User Security Controls
1.8. Physical Security
1.9. Network Controls
1.10. Change Management
1.11. Control of Information
1.12. Logical Security
1.13. Customer Remote Access to Financial Services
1.14. Application Security
1.15. Database Security
1.16. Encryption
1.17. Oversight of Third-Party Service Providers
1.18. Business Continuity Considerations
1.19. Security Operations

1.20. Threat Identification and Assessment
1.21. Incident Identification and Assessment
1.22. Security Program Assurance and Testing

Recommended documentation includes:

- [ ] **Security Program Planning Policy**
- [ ] **Security Program Planning Procedure**
- [ ] Control Evidence Document for each Security Program Planning defined control
- [ ] Roles and responsibilities matrix
- [ ] Risk assessment
- [ ] Risk assessment results
- [ ] Vulnerability scanning schedule
- [ ] Vulnerability remediation schedule
- [ ] Vulnerability management metrics
- [ ] Segregation of duties metrics
- [ ] Confidentiality agreements for personnel (template and executed)
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training schedule
- [ ] Security awareness training records
- [ ] Inventory of wireless access points
- [ ] Change management records

- [ ] Configuration management plan
- [ ] System and device baseline configurations
- [ ] Record retention and disposal schedule
- [ ] List of all personnel
- [ ] List of all accounts
- [ ] List of recently terminated personnel
- [ ] List of recently onboarded personnel
- [ ] List of users with remote access
- [ ] Inventory of third-party providers and suppliers
- [ ] Due diligence assessment for third parties
- [ ] Due diligence results for third parties
- [ ] Threat monitoring reports
- [ ] Incident response plan
- [ ] Incident response training materials and training records
- [ ] Incident response test scripts
- [ ] Incident response test report
- [ ] Incident reports (real-world)

2. MANAGEMENT RESPONSIBILITIES

Topics addressed by documentation for this control family should include:

2.1. Governance
2.2. IT Responsibilities and Functions

2.3. Planning IT Operations and Investment
2.4. Other Functions
2.5. IT Risk Management
2.6. Risk Identification
2.7. Risk Measurement
2.8. Risk Mitigation
2.9. Third-Party Management
2.10. Monitoring and Reporting

Recommended documentation includes:

- [ ] **Security Program Management Policy**
- [ ] **Security Program Management Procedure**
- [ ] Control Evidence Document for each Security Program Management defined control
- [ ] Board of directors' responsibilities
- [ ] IT management responsibilities
- [ ] Executive management responsibilities
- [ ] Chief Information Officer/Chief Technology Officer responsibilities
- [ ] Chief Information Security Officer Responsibilities
- [ ] IT line management responsibilities
- [ ] Business unit management responsibilities
- [ ] Human resources (HR) responsibilities
- [ ] Internal audit repressibilities
- [ ] Performance benchmarks
- [ ] Reports of the effectiveness of controls

3. ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS (AIO)

Topics addressed by documentation for this control family should include:

3.1. Board and Senior Management Responsibilities
3.2. Internal Audit, Independent Reviews, and Certification Processes
3.3. Data Governance and Data Management
3.4. IT Asset Management
3.5. Architecture
3.6. Infrastructure
3.7. Operational Controls
3.8. IT Operational Processes
3.9. Service and Support Processes
3.10. Ongoing Monitoring and Evaluation Processes

Recommended documentation includes:

- [ ] **Architecture, Infrastructure and Operations Policy**
- [ ] **Architecture, Infrastructure and Operations Procedure**
- [ ] Control Evidence Document for each AIO defined control
- [ ] Data classification scheme
- [ ] Hardware inventory
- [ ] Software inventory
- [ ] Data inventory
- [ ] Network diagrams
- [ ] Data flow diagrams
- [ ] System and device maintenance records
- [ ] Configuration management plan
- [ ] Vulnerability management plan

- [ ] Backup schedule
- [ ] Results from backup data recovery testing
- [ ] Capacity management records
- [ ] IT and operations key performance indicators
- [ ] Security program control self-assessments

4. BUSINESS CONTINUITY

Topics addressed by documentation for this control family should include:

4.1. Board and Senior Management Responsibilities
4.2. Audit
4.3. Business Impact Analysis
4.4. Risk Assessments
4.5. Business Continuity Strategies
4.6. Resilience
4.7. Business Continuity Plans
4.8. Training
4.9. Exercises and Tests
4.10. Board Reporting

Recommended documentation includes:

- [ ] **Business Continuity Policy**
- [ ] **Business Continuity Procedure**
- [ ] Control Evidence Document for each Business Continuity defined control
- [ ] Business impact analysis results
- [ ] List of critical business functions
- [ ] Business continuity strategy
- [ ] Business continuity plans

- [ ] Business continuity training materials and training records
- [ ] Business continuity test scripts
- [ ] Business continuity test reports
- [ ] Business continuity report to the Board

5. DEVELOPMENT AND ACQUISITION SECURITY

Topics addressed by documentation for this control family should include:

5.1. Project Management
5.2. Development Procedures
5.3. Acquisition Procedures
5.4. Maintenance Procedures

Recommended documentation includes:

- [ ] **Development and Acquisition Security Policy**
- [ ] **Development and Acquisition Security Procedure**
- [ ] Control Evidence Document for each Development and Acquisition Security defined control

6. OUTSOURCING TECHNOLOGY SERVICES

Topics addressed by documentation for this control family should include:

6.1. Board and Management Responsibilities
6.2. Risk Assessment and Requirements
6.3. Service Provider Selection
6.4. Contract Issues
6.5. Ongoing Monitoring
6.6. Business Continuity Planning

Recommended documentation includes:

- [ ] **Outsourcing Technology Services Policy**

- [ ] **Outsourcing Technology Services Procedure**
- [ ] Control Evidence Document for each Outsourcing Technology Services defined control

7. E-BANKING SECURITY

Topics addressed by documentation for this control family should include:

7.1. Board and Management Oversight
7.2. Managing Outsourcing Relationships
7.3. Security Program Requirements
7.4. Administrative Controls
7.5. Legal and Compliance Issues

Recommended documentation includes:

- [ ] **E-Banking Security Policy**
- [ ] **E-Banking Security Procedure**
- [ ] Control Evidence Document for each E-Banking defined control
- [ ] E-Banking audit reports
- [ ] Due diligence results for outsourcing solutions
- [ ] Contracts for third-party services

8. RETAIL PAYMENT SYSTEM SECURITY

Topics addressed by documentation for this control family should include:

8.1. Retail Payment Systems Risk Management
8.2. Audit
8.3. Security Program Controls
8.4. Business Continuity Planning
8.5. Retail Payment Instrument Specific Risk Management Controls

Recommended documentation includes:

☐ **Retail Payment System Security Policy**

☐ **Retail Payment System Security Procedure**

☐ Control Evidence Document for each Retail Payment System Security defined control

9. WHOLESALE PAYMENT SYSTEM SECURITY

Topics addressed by documentation for this control family should include:

9.1. Internally Developed and Off-the-Shelf Funds Transfer Systems

Recommended documentation includes:

☐ **Wholesale Payment System Security Policy**

☐ **Wholesale Payment System Security Procedure**

☐ Control Evidence Document for each Wholesale Payment System Security defined control

10. AUDITING

Topics addressed by documentation for this control family should include:

10.1. Internal Audit Program
10.2. Risk Assessment and Risk-Based Auditing
10.3. Audit Participation in Application Development, Acquisition, Conversions, and Testing
10.4. Outsourcing Internal IT Audit

Recommended documentation includes:

☐ **Auditing Policy**

☐ **Auditing Procedure**

☐ Control Evidence Document for each defined auditing control

☐ Internal Audit Plan

- [ ] Risk scoring system
- [ ] Internal audit reports

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.