Documentation Checklist for HITRUST

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 HITRUST 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.

HITRUST is comprised of 14 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. SECURITY PROGRAM MANAGEMENT

Topics addressed by documentation for this control family should include:

1.1. Implementing an Effective Security Program

Recommended documentation includes:

- ☐ **Security Program Management Policy**
- ☐ **Security Program Management Procedure**
- ☐ Control Evidence Document for each Security Program Management defined control
- ☐ Security Program Plan

2. ACCESS CONTROL

Topics addressed by documentation for this control family should include:

2.1. Access Control Requirements
2.2. Access Authorizations for Information Systems
  2.2.1. User Registration
  2.2.2. Privilege Management
  2.2.3. User Password Management

2.2.4. Review of User Access Rights
2.3. User Responsibilities
2.3.1. Password Use
2.3.2. Unattended User Equipment
2.3.3. Clean Desk and Clear Screen Controls
2.4. Network Access Control
2.4.1. Use of Network Services
2.4.2. User Authentication for External Connections
2.4.3. Equipment Identification in Networks
2.4.4. Remote Diagnostic and Configuration Port Protection
2.4.5. Segregation in Networks
2.4.6. Network Connection Controls
2.4.7. Network Routing Control
2.5. Operating System Access Control
2.5.1. Secure Logon Processes
2.5.2. User Identification and Authentication
2.5.3. Password Management
2.5.4. Use of System Utilities
2.5.5. Session Timeouts
2.5.6. Connection Time Limitations
2.6. Application and Information Access Control
2.6.1. Information Access Restrictions
2.6.2. Sensitive System Isolation
2.7. Mobile Computing and Working Remotely
2.7.1. Mobile Computing and Communications
2.7.2. Working Remotely

Recommended documentation includes:

- [ ] **Access Control Policy**
- [ ] **Access Control Procedure**
- [ ] Control Evidence Document for each Access Control defined control
- [ ] List of all users and associated permissions
- [ ] Evidence of account and access reviews/audits

- [ ] List of recently terminated personnel
- [ ] List of recently onboarded personnel
- [ ] Network diagrams (depicting segregation of assets)

3. PERSONNEL SECURITY

Topics addressed by documentation for this control family should include:

3.1. Prior to Employment
3.2. Onboarding Personnel
3.3. Terms and Conditions of Employment
3.4. During Employment
3.5. Management Responsibilities
3.6. Disciplinary Process
3.7. Security Awareness Training
3.8. Termination of Employment and Personnel Transfers

Recommended documentation includes:

- [ ] **Personnel Security Policy**
- [ ] **Personnel Security Procedure**
- [ ] Control Evidence Document for each Personnel Security defined control
- [ ] Roles and responsibilities matrix
- [ ] Terms and conditions of employment
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training records
- [ ] Disciplinary/personnel sanction process
- [ ] Exit interview checklist

4. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

4.1. Risk Management Program
4.2. Risk Assessments
4.3. Risk Mitigation
4.4. Risk Evaluation

Recommended documentation includes:

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

5. SECURITY PROGRAM POLICIES

Topics addressed by documentation for this control family should include:

5.1. Developing Security Policies and Procedures
5.2. Reviewing and Updating Security Policies and Procedures

Recommended documentation includes:

- [ ] **Security Program Controls Policy**
- [ ] **Security Program Controls Procedure**
- [ ] Control Evidence Document for each Security Program Policies defined control
- [ ] Evidence of policy and procedure reviews and updates

6. SECURITY PROGRAM STRUCTURE

Topics addressed by documentation for this control family should include:

- 6.1. Internal Organization of the Security Program
  - 6.1.1. Management Commitment to the Security Program
  - 6.1.2. Security program Coordination
  - 6.1.3. Allocation of Security Program Responsibilities
  - 6.1.4. Authorization Process for Information Assets and Facilities
  - 6.1.5. Confidentiality Agreements
  - 6.1.6. Contact with Authorities, Security Groups, and Associations
  - 6.1.7. Independent Reviews of the Security Program
- 6.2. Managing Relationships with External Parties
  - 6.2.1. Identification of Risks Related to External Parties
  - 6.2.2. Addressing Security When Dealing with Customers
  - 6.2.3. Addressing Security in Third Party Agreements

Recommended documentation includes:

- [ ] **Security Program Structure Policy**
- [ ] **Security Program Structure Procedure**
- [ ] Control Evidence Document for each Security Program Structure defined control
- [ ] Security program roles and responsibilities matrix
- [ ] Confidentiality or non-disclosure template
- [ ] Contact and contact information for authorities, security groups, and associations
- [ ] Reports from independent reviews of the Security program
- [ ] Defined security controls for dealing with customers
- [ ] Defined security controls for dealing with third-party providers

7. SECURITY PROGRAM COMPLIANCE

Topics addressed by documentation for this control family should include:

- 7.1. Compliance with Legal Requirements
  - 7.1.1. Identification of Applicable Legislation
  - 7.1.2. Intellectual Property Rights
  - 7.1.3. Protection of Organizational Records
  - 7.1.4. Data Protection and Privacy for Covered Information
  - 7.1.5. Prevention of Misuse of Information Assets
  - 7.1.6. Regulation of Cryptographic Controls
- 7.2. Compliance with Security Program Controls and Technical Requirements
  - 7.2.1. Compliance with Security Policies and Procedures
  - 7.2.2. Technical Compliance Verification
- 7.3. Information System Audit Considerations
  - 7.3.1. Information System Audit Controls
  - 7.3.2. Protection of Information System Audit Tools

Recommended documentation includes:

- ☐ **Security Program Compliance Policy**
- ☐ **Security Program Compliance Procedure**
- ☐ Control Evidence Document for each Security Program Compliance defined control
- ☐ List of application legislation and regulations
- ☐ Defined intellectual property rights, if any.
- ☐ Technical compliance verification reports

8. ASSET MANAGEMENT

Topics addressed by documentation for this control family should include:

- 8.1. Asset Inventory
- 8.2. Acceptable Use of Assets
- 8.3. Asset Classifications
- 8.4. Asset Labeling and Handling Requirements

Recommended documentation includes:

- [ ] **Asset Management Policy**
- [ ] **Asset Management Procedure**
- [ ] Control Evidence Document for each Asset Management defined control
- [ ] Hardware asset inventory
- [ ] Software asset inventory
- [ ] Acceptable use requirements
- [ ] Data classification scheme

9. PHYSICAL SECURITY

Topics addressed by documentation for this control family should include:

9.1. Physical Security Perimeters
9.2. Physical Entry Controls
9.3. Securing Offices, Rooms, and Facilities
9.4. Portion from External and Environmental Threats
9.5. Working in Secure Areas
9.6. Public Access, Delivery, and Loading Areas
9.7. Equipment Locations and Protection
9.8. Supporting Utilities
9.9. Cabling Security
9.10. System and Device Maintenance
9.11. Security of Equipment Off-Premises
9.12. Secure Disposal or Re-Use of Equipment
9.13. Removal of Organizational Property

Recommended documentation includes:

- [ ] **Physical Security Policy**
- [ ] **Physical Security Procedure**

- [ ] Control Evidence Document for each Physical Security defined control
- [ ] List of names and locations of secure areas
- [ ] System and device maintenance records
- [ ] Certificates of destruction for destroyed assets

10. COMMUNICATIONS AND OPERATIONS MANAGEMENT

Topics addressed by documentation for this control family should include:

- 10.1. Documented Operating Procedures
- 10.2. Change Management
- 10.3. Segregation of Duties
- 10.4. Separation of Production and Non-Production Environments
- 10.5. Managing Third Party Service Delivery
  - 10.5.1. Monitoring and Reviewing Third-Party Services
  - 10.5.2. Managing Changes to Third-Party Services
- 10.6. System Planning and Acceptance
  - 10.6.1. Capacity Management
  - 10.6.2. System Acceptance
- 10.7. Malicious Code Protection
- 10.8. Mobile Code Protection
- 10.9. Information and Configuration Backups
- 10.10. Network Security Management
  - 10.10.1. Network Controls
  - 10.10.2. Security of Network Services
- 10.11. Media Handling
  - 10.11.1. Management of Removable Media
  - 10.11.2. Disposal of Media
  - 10.11.3. Media handling Procedures
  - 10.11.4. Security of System Documentation
- 10.12. Exchange of Information
  - 10.12.1. Information Exchange Controls
  - 10.12.2. Exchange Agreements
  - 10.12.3. Physical media in Transit
  - 10.12.4. Electronic Messaging

10.12.5. Interconnected Business Information Systems
10.13. Electronic Commerce Services
10.13.1. Online Transactions
10.13.2. Publicly Available Information
10.14. Audit Logging and Monitoring
10.14.1. Audit Logging
10.14.2. Monitoring System Use
10.14.3. Protection of Log Information
10.14.4. Administrator and Operator Logs
10.14.5. Fault Logging
10.14.6. Clock Synchronization

Recommended documentation includes:

- [ ] **Communications and Operations Management Policy**
- [ ] **Communications and Operations Management Procedure**
- [ ] Control Evidence Document for each Communications and Operations Management defined control
- [ ] Documented operating procedures
- [ ] Change requests with approval decisions
- [ ] Segregation of duties matrix
- [ ] Network diagram(s) depicting segregation of environments
- [ ] Third-party due diligence assessment
- [ ] Third-party due diligence results
- [ ] List of all information systems
- [ ] System-generated report listing information systems protected with anti-malware software
- [ ] Backup schedule

- [ ] Evidence of backup data recovery testing
- [ ] Media inventory
- [ ] Information exchange agreement (template and executed example)
- [ ] Evidence of reviews performed on publicly available information
- [ ] System-generated list of event types being logged/audited

11. SYSTEMS MANAGEMENT

Topics addressed by documentation for this control family should include:

- 11.1. Security Requirements Analysis and Specifications
- 11.2. Correct Processing in Applications
  - 11.2.1. Input Data Validation
  - 11.2.2. Control of Internal Processing
  - 11.2.3. Message Integrity
  - 11.2.4. Output Data Validation
- 11.3. Managing Cryptography
  - 11.3.1. Use of Cryptographic Controls
  - 11.3.2. Key Management Requirements
- 11.4. Security of System Files
  - 11.4.1. Control of Operational Software
  - 11.4.2. Protection of Test Data
  - 11.4.3. Access to Program Source Code
- 11.5. Security for Development and Support Processes
  - 11.5.1. Change Control Processes
  - 11.5.2. Outsources Software Development
- 11.6. Vulnerability Management

Recommended documentation includes:

- [ ] **Systems Management Policy**
- [ ] **Systems Management Procedure**
- [ ] Control Evidence Document for each Systems Management defined control

- [ ] Security requirements for information systems
- [ ] Controls defined for outsourcing software development
- [ ] Vulnerability Management Plan
- [ ] Vulnerability scanning schedule
- [ ] Vulnerability remediation schedule
- [ ] Vulnerability management metrics

12. INCIDENT MANAGEMENT

Topics addressed by documentation for this control family should include:

12.1. Reporting Security Events and Incidents
12.2. Managing Security Incidents
  12.2.1. Responsibilities and Procedures
  12.2.2. Lessons Learned
  12.2.3. Collection of Evidence

Recommended documentation includes:

- [ ] **Incident Management Policy**
- [ ] **Incident Management Procedure**
- [ ] Control Evidence Document for each Incident Management defined control
- [ ] Incident Response Plan
- [ ] Incident reports
- [ ] Post-incident lessons learned meeting agenda and minutes

13. BUSINESS CONTINUITY

Topics addressed by documentation for this control family should include:

13.1. Security Program Aspects of Business Continuity
13.2. Business Continuity and Risk Assessments
13.3. Business Continuity Plans
13.4. Business Continuity Planning Framework
13.5. Business Continuity Testing and Continuous Improvement

Recommended documentation includes:

- [ ] **Business Continuity Policy**
- [ ] **Business Continuity Procedure**
- [ ] Control Evidence Document for each Business Continuity defined control
- [ ] Business continuity planning framework
- [ ] Business Impact Analysis results
- [ ] Business Continuity Plan(s)
- [ ] Business continuity test scripts and reports

14. DATA PRIVACY

Topics addressed by documentation for this control family should include:

14.1. Transparency
  14.1.1. Privacy Notices
  14.1.2. Openness and Transparency
  14.1.3. Accounting of Disclosures
14.2. Individual Participation
  14.2.1. Consent
  14.2.2. Choice
  14.2.3. Principle Access
14.3. Purpose Specification
14.4. Data Minimization
14.5. Use Limitation

14.5.1. Use and Disclosure
14.5.2. Retention and Disposal
14.6. Data Quality and Integrity
14.6.1. Accuracy and Quality
14.6.2. Participation and Redress
14.6.3. Complaint Management
14.7. Accountability and Auditing
14.7.1. Governance
14.7.2. Privacy Impact Assessment
14.7.3. Privacy Requirements for Contractors and Processors
14.7.4. Privacy Monitoring and Auditing
14.7.5. Privacy Protection Awareness and Training
14.7.6. Privacy Protection Reporting

Recommended documentation includes:

- [ ] **Data Privacy Policy**
- [ ] **Data Privacy Procedure**
- [ ] Control Evidence Document for each Data Privacy defined control
- [ ] Privacy notices
- [ ] Accounting of disclosures
- [ ] Complain management process and associated records
- [ ] Privacy Impact Assessment(s)
- [ ] Privacy requirements defined for contractors and processors
- [ ] Business Associate Agreements (template and executed, if applicable)
- [ ] Privacy monitoring and auditing results
- [ ] Privacy training curriculum
- [ ] Privacy training materials

- [ ] Privacy training records
- [ ] Privacy protection 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.