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 ISO 27001 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.

ISO 27001 is comprised of 14 control families. Additionally, ASCENT has added one additional control family to accommodate the requirements identified prior to Annex A of the international standard. 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. Policy and Procedure
1.2. Security Program Management
1.3. Context of the Organization
1.4. Needs and Expectations of Interested Parties
1.5. Scope of the Security Program
1.6. Management Commitment to the Security Program
1.7. Establishing a Security Program Policy Library
1.8. Security Roles and Responsibilities of Personnel
1.9. Risk Management Program
1.10. Risk Assessments
1.11. Risk Treatment and Mitigation
1.12. Achieving Security Program Objectives
1.13. Security Program Resources
1.14. Competence of Personnel
1.15. Security Program Awareness
1.16. Security Program Communication
1.17. Managing Security Program Documentation
1.18. Operational Planning and Control

1.19. Monitoring, Measurement, Analysis, and Evaluation
1.20. Internal Audit Program
1.21. Management Reviews of the Security Program
1.22. Addressing Nonconformity and Taking Corrective Actions
1.23. Continuous Improvement of the Security Program

Recommended documentation includes:

- [ ] **Security Program Planning Policy**
- [ ] **Security Program Planning Procedure**
- [ ] Control Evidence Document for each defined Security Program Planning control
- [ ] Security program plan
- [ ] Statement of applicability
- [ ] Risk management plan
- [ ] Risk assessment
- [ ] Risk assessment results
- [ ] Internal audit plan
- [ ] Continuous monitoring plan

2. SECURITY CONTROL DOCUMENTATION

Topics addressed by documentation for this control family should include:

2.1. Policy and Procedure
2.2. Implementing Security Program Policies
2.3. Reviewing and Updating Security Program Policies

Recommended documentation includes:

- [ ] **Security Control Documentation Policy**

☐ **Security Control Documentation Procedure**

☐ Control Evidence Document for each defined Security Control Documentation control

3. SECURITY PROGRAM STRUCTURE

Topics addressed by documentation for this control family should include:

3.1. Policy and Procedure
3.2. Internal Organization of the Security Program
3.3. Segregation of Duties
3.4. Contact with Authorities, Security Groups, and Associations
3.5. Project Management Security Requirements
3.6. Mobile Computing and Working Remotely

Recommended documentation includes:

☐ **Security Program Structure Policy**

☐ **Security Program Structure Procedure**

☐ Control Evidence Document for each defined Security Program Structure control

☐ Segregation of duties matrix

☐ Contacts and contact information for authorities, security groups, and associations

4. PERSONNEL SECURITY

Topics addressed by documentation for this control family should include:

4.1. Policy and Procedure
4.2. Personnel Screening
4.3. Terms and Conditions of Employment
4.4. Management Responsibilities
4.5. Security Awareness Training
4.6. Disciplinary Process

4.7. Termination of Employment and Personnel Transfers

Recommended documentation includes:

- [ ] **Personnel Security Policy**
- [ ] **Personnel Security Procedure**
- [ ] Control Evidence Document for each defined Personnel Security control
- [ ] Personnel screening criteria
- [ ] Terms and conditions of employment
- [ ] Security awareness training materials
- [ ] Security awareness training records
- [ ] Exit interview checklist for personnel

5. ASSET MANAGEMENT

Topics addressed by documentation for this control family should include:

5.1. Policy and Procedure
5.2. Asset Inventory
5.3. Acceptable Use of Assets
5.4. Return of Assets
5.5. Classification, Labeling, and Handling of Information Assets
5.6. Media Handling and Protection

Recommended documentation includes:

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

☐ Acceptable use requirements / Rules of behavior

6. ACCESS CONTROL

Topics addressed by documentation for this control family should include:

6.1. Policy and Procedure
6.2. Access Control Requirements
6.3. Account Management
6.4. Privilege Management
6.5. Access Reviews
6.6. Access Revocation and Modification
6.7. Password Management
6.8. Access Controls for Systems and Applications
6.9. Secure Logon Process
6.10. Controlling the Use of System Utilities
6.11. Restricting Access to Source Code

Recommended documentation includes:

☐ **Access Control Policy**

☐ **Access Control Procedure**

☐ Control Evidence Document for each defined Access Control requirement

☐ Account and permission review/audit report

☐ List of all users

☐ List of recently terminated personnel

☐ List of recently onboarded personnel

☐ RBAC matrix

7. CRYPTOGRAPHY

Topics addressed by documentation for this control family should include:

7.1. Policy and Procedure
7.2. Cryptographic Controls

Recommended documentation includes:

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

8. PHYSICAL SECURITY

Topics addressed by documentation for this control family should include:

8.1. Policy and Procedure
8.2. Maintaining Secure Areas
8.3. External and Environmental Threat Protection
8.4. Equipment Placement and Protection
8.5. Managing Supporting Utilities
8.6. Cabling Security
8.7. Equipment Maintenance
8.8. Security of Assets While Off-Premises
8.9. Secure Disposal or Re-Use of Information Assets
8.10. Unattended Information Systems

Recommended documentation includes:

- [ ] **Physical Security Policy**
- [ ] **Physical Security Procedure**
- [ ] Control Evidence Document for each defined Physical Security control
- [ ] List of secure areas
- [ ] System and device maintenance records

☐ Certificates of destruction

9. OPERATIONS SECURITY

Topics addressed by documentation for this control family should include:

9.1. Policy and Procedure
9.2. Operational Procedures
9.3. Change Management
9.4. Capacity Management
9.5. Separation of Production and Non-Production Environments
9.6. Malware Protection
9.7. Backup Requirements
9.8. Logging and Monitoring
9.9. Protection of Logging Information
9.10. Controlling Operational Software
9.11. Vulnerability Management
9.12. Audit Considerations for Systems and Applications

Recommended documentation includes:

☐ **Operations Security Policy**

☐ **Operations Security Procedure**

☐ Control Evidence Document for each defined Operations Security control

☐ Change requests and approval decisions

☐ Evidence of separation of production and non-production environments

☐ Standard operating procedures

☐ List of all information assets

☐ System-generated report that lists assets protected with anti-malware software

☐ Evidence of backup data recovery testing

☐ Vulnerability remediation metrics

10. COMMUNICATIONS SECURITY

Topics addressed by documentation for this control family should include:

10.1. Policy and Procedure
10.2. Managing the Security of the Network
10.3. Information Transfers
10.4. Securing Electronic Messaging and Internet Use
10.5. Confidentiality or Non-Disclosure Agreements

Recommended documentation includes:

☐ **Communications Security Policy**

☐ **Communications Security Procedure**

☐ Control Evidence Document for each defined Communications Security control

☐ Confidentiality or Non-Disclosure Agreement template and records

11. SYSTEMS MANAGEMENT

Topics addressed by documentation for this control family should include:

11.1. Policy and Procedure
11.2. Security Requirements for Information Systems
11.3. System Development Life Cycle (SDLC)
11.4. Outsourced Development
11.5. System Acceptance and Authorization
11.6. Test Data

Recommended documentation includes:

☐ **Systems Management Policy**

☐ **Systems Management Procedure**

☐ Control Evidence Document for each defined Systems Management control

☐ SDLC process documentation

12. THIRD PARTY DUE DILIGENCE

Topics addressed by documentation for this control family should include:

12.1. Policy and Procedure
12.2. Security Controls for Third Party Provider Relationships
12.3. Third Party Contract Management
12.4. Monitoring Third Party Service Delivery

Recommended documentation includes:

☐ **Third Party Due Diligence Policy**

☐ **Third Party Due Diligence Procedure**

☐ Control Evidence Document for each defined Third-Party Due Diligence control

☐ Inventory of third-party providers and suppliers

☐ Risk ranking of third-party providers and suppliers

☐ Due Diligence assessment results

13. INCIDENT MANAGEMENT

Topics addressed by documentation for this control family should include:

13.1. Policy and Procedure
13.2. Management of Incidents and Continuous Improvements
13.3. Reporting Security Events and Incidents
13.4. Incident Triage
13.5. Incident Response Plan
13.6. Lessons Learned and Continuous Improvement
13.7. Collection of Evidence

Recommended documentation includes:

☐ **Incident Response Policy**

- [ ] **Incident Response Procedure**
- [ ] Control Evidence Document for each defined Incident Response control
- [ ] Incident Response Plan
- [ ] Incident reports

14. BUSINESS CONTINUITY

Topics addressed by documentation for this control family should include:

14.1. Policy and Procedure
14.2. Security Program Continuity
14.3. Business Continuity Testing and Training
14.4. System and Infrastructure Redundancies

Recommended documentation includes:

- [ ] **Business Continuity Policy**
- [ ] **Business Continuity Procedure**
- [ ] Control Evidence Document for each defined Business Continuity control
- [ ] Business Continuity Plans
- [ ] Business continuity test scripts and reports
- [ ] Business continuity training materials
- [ ] Business continuity training records
- [ ] Evidence of critical system and infrastructure redundancies

15. SECURITY PROGRAM COMPLIANCE

Topics addressed by documentation for this control family should include:

15.1. Policy and Procedure

15.2. Compliance with Legal Requirements
15.3. Security Program Reviews

Recommended documentation includes:

- [ ] **Security Program Compliance Policy**
- [ ] **Security Program Compliance Procedure**
- [ ] Control Evidence Document for each defined Security Program Compliance control
- [ ] List of applicable legal and regulatory requirements

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.