Documentation Checklist for GDPR

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 GDPR 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 GDPR security programs, 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. Documented Security Program Plan
1.2. Policies and Procedures
1.3. Management Commitment to the Security Program
1.4. Security Program Roles and Responsibilities
1.5. Management Reviews of the Security Program
1.6. Independent Reviews of the Security Program
1.7. Continuous Monitoring

Recommended documentation includes:

- [ ] **Security Program Planning Policy**
- [ ] **Security Program Planning Procedure**
- [ ] Control Evidence Documents for all Security Program Planning controls
- [ ] Security program assessment process
- [ ] Exception Management Procedure
- [ ] Exception Request form Template

- [ ] Corrective Action Plan template
- [ ] Continuous Monitoring Plan

2. RISK MANAGEMENT

Topics addressed by documentation for this control family should include:

2.1. Policy and Procedure
2.2. Risk Management Strategy
2.3. Risk Management Program
2.4. Risk Assessments
2.5. Risk Treatment and Mitigation
2.6. Security Categorization and Risk Framing
2.7. Supply Chain Risk Management

Recommended documentation includes:

- [ ] **Risk Management Policy**
- [ ] **Risk Management Procedure**
- [ ] Control Evidence Documents for all Risk Management controls
- [ ] Risk management strategy
- [ ] Risk assessment template and report
- [ ] Risk treatment and mitigation process
- [ ] Risk appetite statement
- [ ] System Security Plan

3. PERSONNEL SECURITY

Topics addressed by documentation for this control family should include:

3.1. Policy and Procedure
3.2. Roles and Responsibilities of Personnel

3.3. Personnel Screening
3.4. Terms and Conditions of Employment
3.5. Management Responsibilities
3.6. Disciplinary Process
3.7. Termination or Change of Employment
3.8. Security Awareness Training Program

Recommended documentation includes:

- [ ] **Personnel Security Policy**
- [ ] **Personnel Security Procedure**
- [ ] Control Evidence Documents for all Personnel Security controls
- [ ] Roles and responsibilities matrix for personnel
- [ ] Background screening process
- [ ] Position risk designations
- [ ] Terms and conditions of employment
- [ ] Exit interview process and checklist
- [ ] Personnel transfer process and checklist
- [ ] Security awareness training materials
- [ ] Security awareness training records

4. ASSET MANAGEMENT

Topics addressed by documentation for this control family should include:

4.1. Policy and Procedure
4.2. Asset Inventory
4.3. Acceptable Use of Assets
4.4. Classification, Labeling, and Handling of Assets
4.5. Secure Disposal or Re-Use of Equipment

Recommended documentation includes:

- [ ] **Asset Management Policy**
- [ ] **Asset Management Procedure**
- [ ] Control Evidence Documents for all Asset Management controls
- [ ] Asset inventory
- [ ] Network diagrams
- [ ] Acceptable use requirements and acknowledgements
- [ ] System logon banners
- [ ] Asset disposal and re-user process

5. ACCESS CONTROL

Topics addressed by documentation for this control family should include:

5.1. Policy and Procedure
5.2. Access Control Program
5.3. Account Management
5.4. User Identification and Authentication
5.5. Privilege Management
5.6. Secure Logon Process
5.7. Password Management
5.8. Unattended Equipment
5.9. Controlling the Use of System Utilities
5.10. Session Timeouts and Time of Day Limitations
5.11. Remote Access Management
5.12. Managing Wireless Access
5.13. Segregation in Networks
5.14. Segregation of Duties
5.15. Mobile Computing and Working Remotely

Recommended documentation includes:

- [ ] **Access Control Policy**
- [ ] **Access Control Procedure**
- [ ] Control Evidence Documents for all Access Control controls
- [ ] Role Based Access Control (RBAC) Matrix
- [ ] Evidence of access reviews

6. PHYSICAL SECURITY

Topics addressed by documentation for this control family should include:

6.1. Policy and Procedure
6.2. Physical Security Perimeters
6.3. Physical Entry Controls
6.4. Protection against External and Environmental Threats
6.5. Equipment Placement and Protection
6.6. Managing Supporting Utilities
6.7. Cabling Security
6.8. Security of Information Assets while Off-Premises
6.9. Protection of Physical Media in Transit

Recommended documentation includes:

- [ ] **Physical Security Policy**
- [ ] **Physical Security Procedure**
- [ ] Control Evidence Documents for all Physical Security controls
- [ ] Physical access control list
- [ ] Evidence of physical access control list reviews
- [ ] Evidence of physical access log reviews
- [ ] Physical access device inventory

- [ ] Evidence of combination and key changes

7. OPERATIONS SECURITY

Topics addressed by documentation for this control family should include:

7.1. Policy and Procedure
7.2. Malicious and Mobile Code Protection
7.3. Information and Configuration Backups
7.4. Technical Vulnerability Management
7.5. Audit Logging and Monitoring
7.6. Protection of Log Information
7.7. Flaw Remediation and Fault Logging
7.8. Cybersecurity Controls
7.9. Penetration Testing

Recommended documentation includes:

- [ ] **Operations Security Policy**
- [ ] **Operations Security Procedure**
- [ ] Control Evidence Documents for all Operations Security controls
- [ ] List of all assets
- [ ] System-generated report listing assets with anti-malware software installed
- [ ] Evidence of regular backups being performed
- [ ] Vulnerability management metrics
- [ ] Vulnerability scanning reports
- [ ] Penetration test reports

8. COMMUNICATIONS SECURITY

Topics addressed by documentation for this control family should include:

8.1. Policy and Procedure
8.2. Network Security Controls
8.3. Protecting the Exchange of Information
8.4. Electronic Messaging and Internet Use Protection
8.5. Cryptography
8.6. Publicly Available Information

Recommended documentation includes:

- [ ] **Communications Security Policy**
- [ ] **Communications Security Procedure**
- [ ] Control Evidence Documents for all Communications Security controls
- [ ] Evidence of publicly accessible information reviews

9. SYSTEMS MANAGEMENT

Topics addressed by documentation for this control family should include:

9.1. Policy and Procedure
9.2. Separation of Non-Production and Production Environments
9.3. System Development Lifecycle
9.4. System Development and Acquisition
9.5. Outsourced Development and External System Services
9.6. Infrastructure Management
9.7. Control of Operational Software
9.8. Configuration Management Plan
9.9. Baseline Configurations of System and Devices
9.10. Change Management
9.11. Capacity Management
9.12. System and Device Maintenance
9.13. System Documentation

Recommended documentation includes:

- [ ] **Systems Management Policy**
- [ ] **Systems Management Procedure**
- [ ] Control Evidence Documents for all Systems Management controls
- [ ] SDLC process documentation
- [ ] List of installed software
- [ ] Interconnection Security Agreement template
- [ ] Configuration Management Plan
- [ ] Baseline System and Device Configurations
- [ ] Change management process

10. THIRD PARTY DUE DILIGENCE

Topics addressed by documentation for this control family should include:

10.1. Policy and Procedure
10.2. Identifying Risks Related to External Parties
10.3. Addressing Security in Third-Party Agreements
10.4. Third Party Contract Management
10.5. Third Party Due Diligence
10.6. Monitoring Third Party Services

Recommended documentation includes:

- [ ] **Third Party Due Diligence Policy**
- [ ] **Third Party Due Diligence Procedure**
- [ ] Control Evidence Documents for all Third-Party Due Diligence controls
- [ ] Preliminary Assessment questionnaire
- [ ] Due diligence assessment questionnaire and report template

- [ ] Inventory of current third-party providers and suppliers
- [ ] Standard contractual security requirements for third parties

11. INCIDENT RESPONSE

Topics addressed by documentation for this control family should include:

11.1. Policy and Procedure
11.2. Incident Response Planning and Preparation
11.3. Contact with Authorities, Security Groups, and Associations
11.4. Reporting Security Events and Incidents
11.5. Incident Handling
11.6. Incident Detection and Identification
11.7. Incident Triage
11.8. Incident Containment and Mitigation
11.9. Incident Communications and Reporting
11.10. Incident Response Plan
11.11. Incident Response Testing and Training
11.12. Lessons Learned Reviews

Recommended documentation includes:

- [ ] **Incident Response Policy**
- [ ] **Incident Response Procedure**
- [ ] **Incident Response Plan**
- [ ] Control Evidence Documents for all Incident Response controls
- [ ] Incident response report template
- [ ] Incident response testing scenarios and results
- [ ] Incident response training materials
- [ ] Incident response training records

12. BUSINESS CONTINUITY

Topics addressed by documentation for this control family should include:

12.1. Policy and Procedure
12.2. Business Continuity Planning
12.3. Business Impact Analysis
12.4. Alternate Processing and Storage Sites
12.5. Business Continuity Testing and Training

Recommended documentation includes:

- [ ] **Business Continuity Policy**
- [ ] **Business Continuity Procedure**
- [ ] **Business Continuity Plans**
- [ ] Control Evidence Documents for all Business Continuity controls
- [ ] Business continuity testing scenarios and results
- [ ] Business continuity training materials
- [ ] Business continuity training reports

13. DATA PRIVACY

Topics addressed by documentation for this control family should include:

13.1. Policy and Procedure
13.2. Transparency
  13.2.1. Privacy Notice
  13.2.2. Accounting of Disclosures
13.3. Individual Participation
  13.3.1. Consent
  13.3.2. Choice
  13.3.3. Principle Access
13.4. Purpose Specification
13.5. Data Minimization
13.6. Use Limitation

13.6.1. Use and Disclosure
13.6.2. Retention and Disposal
13.7. Data Quality and Integrity
13.7.1. Accuracy and Quality
13.7.2. Participation and Redress
13.7.3. Complaint Management
13.8. Accountability and Auditing
13.8.1. Governance
13.8.2. Privacy Impact Assessments
13.8.3. Privacy Requirements for Contractors and Processes
13.8.4. Privacy Monitoring and Auditing
13.8.5. Privacy Protection Awareness and Training
13.8.6. Privacy Protection Reporting

Recommended documentation includes:

- [ ] **Data Privacy Policy**
- [ ] **Data Privacy Procedure**
- [ ] Control Evidence Documents for all Data Privacy controls
- [ ] Information Sharing Agreement template
- [ ] Complaint management process
- [ ] External facing privacy notice(s)
- [ ] Privacy Impact Assessments
- [ ] Privacy awareness training curriculum
- [ ] Privacy awareness training materials
- [ ] Privacy awareness training records

14. SECURITY PROGRAM COMPLIANCE

Topics addressed by documentation for this control family should include:

14.1. Policy and Procedure
14.2. Compliance with Legal Requirements
14.3. Compliance with Policy, Procedure, and Technical Requirements
14.4. Records Retention

Recommended documentation includes:

- [ ] **Security Program Compliance Policy**
- [ ] **Security Program Compliance Procedure**
- [ ] Control Evidence Documents for all Security Program Compliance controls
- [ ] Record retention schedule
- [ ] Confidentiality or Non-Disclosure Agreement template

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.