SOFEMA
AVIATION SERVICES

Basic Check List for ISO 27001 Cyber Security Information System

Provided by Sofema Aviation Services (SAS) www.sassofia.com

The field of information security is increasingly critical in our digital world, where data breaches and cyber threats are becoming more sophisticated. To address these challenges, organizations are turning to international standards like ISO 27001 to strengthen their information security management systems (ISMS).

Sofema Aviation Services (SAS) is pleased to provide an essential Basic Checklist for ISO 27001 Cyber Security Information System.

This checklist is a pivotal resource for organizations aiming to comply with ISO 27001 standards, offering a structured approach to evaluating and enhancing their cybersecurity posture. It encompasses a wide range of components, from system acquisition and incident management to business continuity and compliance, ensuring a holistic approach to information security.

Consider the following Core System Areas.

- **Information system acquisition, development, and maintenance**
  - Security requirements of information systems
  - Correct processing in applications
  - Cryptographic controls
  - Security of system files
  - Security in development and support services
  - Technical vulnerability management
- **Information security incident management**
  - Reporting information security events and weaknesses
  - Management of information security incidents and improvements
- **Business Continuity Management**
  - Information security aspects of Business continuity management
- **Compliance**
  - Compliance with legal requirements
  - Compliance with technical policies and standards and technical compliance
- **Information system audit considerations**
  - Security Policy Checklist
  - Information Security Policy

Assessment Checklist

This checklist covers various aspects of security policy, organization, asset management, human resources, and physical security.

Each item includes key areas of focus for compliance and effective security management.

This checklist should be used to ensure each area is systematically reviewed and managed according to the organizational security requirements.

- **Existence and approval of Information Security Policy**
  - Management approval
  - Communication to employees
  - Statement of management commitment
- **Review of Information Security Policy**
  - Regular review intervals
  - Policy owner responsibilities
  - Management review procedures
  - Consideration of review results
  - Management approval for revised policy
  - Organization of Information Security
- **Internal Organization**
  - Management commitment to information security
  - Coordination of information security
  - Allocation of responsibilities
  - Authorization process for new facilities
  - Confidentiality agreements
  - Contact with authorities
  - Contact with special interest groups
  - Independent review of information security
  - External Parties
  - Identification of risks related to external parties
  - Security in customer relations
  - Security in third-party agreements
- **Asset Management**
  - Responsibility for Assets
  - Inventory of assets
  - Ownership of assets
  - Acceptable use of assets
  - Information Classification
  - Classification guidelines
  - Information labelling and handling
- **Cyber Risk Assessment Checklist**

- Inventory of all information assets
- Classification of assets based on their importance and sensitivity.
- Threat Identification:
  - Identification of potential threats to each information asset
  - Analysis of threat sources (e.g., natural disasters, malicious attacks, system failures)
- Vulnerability Assessment:
  - Analysis of existing vulnerabilities within the system
  - Regular scanning for new vulnerabilities
- Risk Analysis and Evaluation:
  - Assessment of the likelihood and impact of potential threats exploiting vulnerabilities
  - Prioritization of risks based on their severity.
- Current Security Measures Assessment:
  - Evaluation of existing security measures and their effectiveness
  - Identification of areas lacking sufficient safeguards
- Risk Treatment Plan:
  - Development of strategies to mitigate, transfer, accept, or avoid risk
  - Creation of an action plan for implementation of risk treatment strategies
- Incident Response and Recovery Plan:
  - Establishment of an incident response plan
  - Development of a recovery plan to maintain business continuity post-incident.
- Compliance and Legal Requirements:
  - Review of compliance with relevant laws, regulations, and standards
  - Ensuring risk assessment processes meet legal and regulatory requirements.
- Regular Review and Update of Risk Assessment:
  - Periodic review and update of the risk assessment
  - Adaptation to changes in the threat landscape, business processes, or technology.
- Documentation and Reporting:
  - Comprehensive documentation of the risk assessment process
  - Reporting of findings to relevant stakeholders for informed decision-making

- **Human Resources Security**
  - Prior to Employment
  - Roles and responsibilities
  - Screening

  - Terms and conditions of employment
  - During Employment
  - Management responsibilities
  - Security awareness training
  - Disciplinary process
  - Termination/Change of Employment
  - Termination responsibilities
  - Return of assets
  - Removal of access rights
- **Physical and Environmental Security (Secure Areas)**
  - Physical security perimeter
  - Physical entry controls
  - Securing offices and facilities
  - Protection from threats
  - Working in secure areas
  - Public access and delivery areas
- **Physical and Environmental Security (Equipment Security)**
  - Equipment siting and protection
  - Supporting utilities
  - Cabling security
  - Equipment maintenance
  - Security of equipment off-premises
  - Disposal or reuse of equipment
  - Removal of property
- **Communication and Operations Management**
  - Documented Operating Procedures
    - Are operating procedures documented, maintained, and available?
    - Are changes to procedures formally managed?
  - Change Management
    - Is there control over changes to information systems and facilities?
  - Segregation of Duties
    - Are duties and responsibilities separated to minimize unauthorized activities?
- **Separation of Environments**
  - Are development, test, and operational environments isolated?
- **Third-party Service Management**
  - Are third-party security controls and service levels implemented and monitored?
  - Is third-party service provision and change managed considering risk?
- **System Planning and Acceptance**

  - Are capacity demands monitored and projected?
  - Are new systems and upgrades subject to acceptance testing?
  - Protection Against Malicious and Mobile Code
  - Are controls against malicious and mobile code in place?
- **Backup**
  - Are regular backups and tests conducted according to policy?
- **Network Security Management**
  - Is network managed to protect information and control security features?
- **Media Handling**
  - Are removable media managed and disposed of securely?
- **Exchange of Information**
  - Are policies and procedures for secure information exchange in place?
- **Electronic Commerce Services**
  - Is e-commerce information protected and secured?
- **Monitoring**
  - Are audit logs, system use, and faults monitored and protected?
  - Access Control Checklist
  - Access Control Policy
  - Is there an access control policy reviewed based on business requirements?
- **User Access Management**
  - Are user registration and de-registration procedures formalized?
  - Is privilege management controlled and reviewed?
- **User Responsibilities**
  - Are there secure password practices and policies for unattended equipment?
- **Network Access Control**
  - Are network services and connection controls in place and authenticated?
- **Operating System Access Control**
  - Are secure log-on procedures and user authentication enforced?
- **Application and Information Access Control**
  - Are information access restrictions aligned with access control policy?
- **Mobile Computing and Teleworking**
  - Is there a policy for mobile computing and teleworking?
- **Security Requirements**
  - Are security requirements integrated into system projects?
- **Correct Processing in Applications**
  - Is input, processing, and output data validated within applications?
- **Cryptographic Controls**
  - Is there a policy and key management for cryptographic controls?

- **Security of System Files**
  - Are controls in place for operational software, test data, and source code?
- **Security in Development and Support Services**
  - Are change control procedures and outsourced development managed securely?
- **Technical Vulnerability Management**
  - Is information on technical vulnerabilities obtained and acted upon?
  - Information Security Incident Management Checklist
- **Reporting Security Events**
  - Are security events and weaknesses reported and managed effectively?
- **Incident Management**
  - Are responsibilities and procedures for incident management established?
- **Collection of Evidence**
  - Is evidence collected following procedures compliant with legal standards?
- **Business Continuity Management Process**
  - Is there a process to address security for business continuity?
- **Business Continuity Planning**
  - Are continuity plans developed, tested, and maintained?
- **Legal Compliance**
  - Are legal, regulatory, and contractual requirements identified and met?
- **Compliance with Security Policies and Standards**
  - Is compliance with security policies and standards regularly reviewed?
- **Information Systems Audit Considerations**
  - Are information system audit activities planned to minimize disruption?

The Basic Checklist for ISO 27001 Cyber Security Information System provided by Sofema Aviation Services is an invaluable tool for organizations seeking to establish, implement, maintain, and continually improve their information security management system.

- The checklist not only guides the assessment of various aspects of security policy and organization but also helps in systematically managing these components in alignment with organizational security requirements.
- By adhering to this checklist, organizations can ensure they are on the right path towards achieving ISO 27001 compliance, ultimately leading to a more secure and resilient information infrastructure.
- This proactive approach is essential in today's digital landscape, where safeguarding information assets is not just a regulatory requirement but a fundamental aspect of sustaining trust and integrity in the digital ecosystem.

Next Steps

For Additional information or to enrol for a Cyber Security Training Please see www.sassofia.com www.sofemaonline.com or email team@sassofia.com

Please see the following course available online with www.sofemaonline.com

EASA Compliant Organization Cyber Security Responsibilities
https://sofemaonline.com/lms/all-courses/458-easa-compliant-organization-cyber-security-responsibilities/preview