SOFEMA
AVIATION SERVICES

Aviation Operations Information & Cyber Security Compliance Checklist & Risk Assessment Guidance.

Sofema Aviation Services (SAS) Provides the following Guidance Document to support evaluation and implementation of the ISMS.

Reference: Regulation (EU) 2023/203, 2022/1645, and ED Decisions 2023/008–010

Part 1 - Glossary of Terms

BIA – Business Impact Analysis
A method used to find out which systems or processes are most critical to the organization and what would happen if they were disrupted.

Blockchain / Hash Logs
Secure systems that record changes in a way that makes tampering obvious or impossible. Used to protect important records, such as cargo manifests.

Brute-Force Protection
Security tools that stop attackers from guessing passwords by trying thousands of combinations quickly (e.g., by locking accounts after repeated failures).

CAPTCHA – Completely Automated Public Turing test to tell Computers and Humans Apart
Tools that help websites distinguish between real users and automated bots (e.g., clicking images or typing letters from an image).

Cyber Hygiene
Daily habits that help protect against cyber risks, like updating software, using strong passwords, and avoiding suspicious links.

Cybersecurity Incident Logging
Recording security-related events and system activity, including what happened, when, and who was involved—important for investigations and audits.

Data Loss Prevention (DLP)
Tools and techniques used to stop sensitive information (like passenger names or payment info) from being sent outside the organization without approval.

Data Minimization
A privacy rule that says organizations should collect only the data they really need—and only keep it for as long as necessary.

Digital Signature
A secure way to sign electronic documents to prove who signed them and ensure the document hasn't been changed.

EFB – Electronic Flight Bag
A tablet or software used by pilots to access flight manuals, charts, and dispatch info. Needs protection to prevent tampering or data loss.

Encryption (TLS/SSL)
A method of scrambling data so only the intended recipient can read it. TLS/SSL protects information sent over the internet (like bookings or payments).

ISO/IEC 27001
An international standard that helps organizations set up and run an information security management system (ISMS).

ISO/IEC 27005
A guide on how to assess information security risks and decide what to do about them, often used alongside ISO/IEC 27001.

ISMS – Information Security Management System
A structured way to manage and improve information security using people, processes, and technology. It helps protect systems and data from threats.

NIST CSF – National Institute of Standards and Technology Cybersecurity Framework
A global reference framework used to manage cybersecurity risks. It covers five steps: Identify, Protect, Detect, Respond, and Recover.

OWASP – Open Web Application Security Project
A group that identifies the most common website security issues and publishes best practices, such as the "OWASP Top 10."

Payment Card Industry Data Security Standard (PCI-DSS)
Rules that apply to any company processing credit cards. They help protect payment data during transactions.

Phishing
A cyberattack where someone tries to trick users into giving away sensitive information, like passwords, usually by email or fake websites.

Principle of Least Privilege (PoLP)
The idea that employees should have only the minimum access they need to do their job. This reduces the risk of misuse.

Ransomware Containment Readiness
Plans and measures to stop ransomware attacks (where data is encrypted and held for ransom) from spreading and to restore systems.

Residual Risk
Any remaining risk after security measures have been put in place. Must be reviewed and accepted by management.

Risk Acceptability Criteria
Guidelines set by an organization to decide which risks are tolerable and which need to be reduced or eliminated.

Runbooks
Step-by-step emergency guides for handling cybersecurity events or system failures, helping staff respond quickly and consistently.

Security Operations Center (SOC)
A team or office that monitors IT systems for signs of attacks and coordinates the response to cybersecurity incidents.

Tokenization
A security process that replaces sensitive data, like credit card numbers, with a random string (a token) that's meaningless if stolen.

Transport Layer Security / Secure Sockets Layer (TLS/SSL)
Encryption technologies that keep data safe when it travels over the internet. TLS is the modern version; SSL is older.

UEBA – User and Entity Behavior Analytics
Software that watches for strange or suspicious activity from users or systems that might suggest a cybersecurity issue or insider threat.

WAF – Web Application Firewall
A tool that protects websites by filtering out harmful traffic, such as hacking attempts or malicious software.

Whistleblowing / Behavioral Anomaly Reporting
Systems that let employees confidentially report suspicious behavior or cybersecurity issues. Often used to detect insider threats.

Part 2 - Establishment of an Information Security Management System (ISMS)

- Has an ISMS been formally implemented across the organisation in line with IS.I.OR.200?
- Is the ISMS integrated with the Safety Management System (SMS) where applicable?
- Has top management endorsed the ISMS policy, ensuring alignment with organisational objectives?
- Are defined roles and responsibilities established for the ISMS?

Identification of Information Assets and Dependencies

- Are critical information assets and supporting services identified and documented?
- Are dependencies on third-party services clearly identified (e.g., cloud providers, suppliers)?
- Has a business impact analysis (BIA) been conducted?

Risk Assessment and Classification (see Part 2)

- Is a documented risk assessment methodology in place?
- Are threats assessed in terms of their impact on aviation safety and operations?
- Is the risk assessment reviewed periodically (at least annually or after significant change)?
- Are risk acceptability criteria established and approved by management?

Risk Treatment and Mitigation Planning

- Are mitigations documented for each identified risk?
- Have residual risks been reviewed and accepted by the accountable manager?
- Is there evidence of implementation of protective measures (e.g., firewall, encryption, access control)?

Security Controls Implementation

- Are baseline controls implemented according to Annex IS.I.OR.200 and AMC/GM?
- Do implemented controls reflect industry standards such as ISO/IEC 27001 and NIST CSF?
- Are logical and physical access controls in place and tested?

Detection, Response & Recovery Capability

- Are systems and procedures in place to detect and report security events?
- Is there an incident response plan that includes containment, eradication, and recovery?
- Are backups regularly taken and tested for recovery?

- Are incident logs maintained in line with IS.I.OR.200(e) and IS.AR.215?

Supply Chain & Contractor Oversight

- Are contractual provisions in place for cybersecurity in contracts with third parties?
- Are suppliers audited periodically for cybersecurity compliance?
- Is there a process for managing third-party risks, especially for critical services?

Personnel Competence & Awareness

- Have all staff received cybersecurity awareness training appropriate to their role?
- Is advanced training provided to IT, compliance, and safety-critical staff?
- Is there a periodic training refresh and competency validation program?

Security Governance and Continuous Improvement

- Is there regular management review of ISMS effectiveness?
- Are non-conformities tracked, investigated, and resolved?
- Are lessons learned from incidents or external reports integrated into the ISMS?
- Is continuous improvement documented and demonstrated per IS.I.OR.235?

Record Keeping and Audit Trail

- Are ISMS activities (assessments, decisions, treatments) documented and archived?
- Is there a record-keeping policy for logs, reports, and audit trails?
- Is retention in line with regulatory and business requirements?

Coordination with National Authorities (NIS Reporting)

- Is a process in place to notify NIS competent authorities of major cybersecurity incidents?
- Are data breach thresholds and reporting timelines defined?
- Are reporting responsibilities clearly assigned?

Compliance with Associated Regulations

- Are amendments to EU 1321/2014, 965/2012, and 748/2012 incorporated into internal compliance programs?
- Has the organisation evaluated its readiness for applicability dates and transition provisions?

Monitoring and Review

- Are key performance indicators (KPIs) for information security defined and monitored?
- Are security audits conducted at regular intervals, including internal and external reviews?
- Are findings from audits tracked to closure?

Part 3 - Cybersecurity Risk Evaluation Framework by Operational Domain

Recommended Methodology to address Information & Cyber Security Risk

Step 1: Map digital assets and services in each area.
Step 2: Classify each asset/service based on its impact on safety, continuity, and compliance.
Step 3: Evaluate threats, vulnerabilities, and likelihood using ISO 27005 or NIST CSF.
Step 4: Document existing controls and identify gaps.
Step 5: Assign risk ratings and define mitigation/treatment plans.
Step 6: Review periodically and after incidents/changes.

Flight Operations

Aspects:
- Electronic Flight Bag (EFB)
- Aircraft connectivity (ACARS, SATCOM, Wi-Fi)
- Flight planning and dispatch systems

Elements:
- Integrity of flight plans
- Unauthorized changes to navigation data
- Disruption of flight deck comms/data exchange

Criteria:
- Authentication and access controls on pilot systems
- Encryption of comms with OCC
- EFB app validation and update control

Ground Operations

Aspects:
- Airside coordination systems
- Ramp resource management (scheduling, marshalling)

Elements:
- Equipment tracking and vehicle coordination
- Data integrity of work orders and GSE allocation

Criteria:
- System access logs and privileges
- Vulnerability assessment of scheduling systems

- Backup communications and failover strategy

Passenger Services

Aspects:
- Reservation and check-in systems
- Baggage tracking and biometric boarding

Elements:
- PII protection (passport, booking, travel data)
- Boarding systems (gate integration)

Criteria:
- Role-based access control (RBAC) and multifactor auth
- Data loss prevention (DLP) for customer systems
- Real-time monitoring of queueing/processing systems

Cargo and Dangerous Goods (DG)

Aspects:
- Cargo acceptance and manifesting
- DG declaration and classification systems

Elements:
- Manifest tampering risk
- Hazardous material misdeclaration

Criteria:
- Blockchain or hash logs for manifest integrity
- Verification processes for DG declarations
- Access audit trail for warehouse and cargo data systems

Maintenance (CAMO & AMO)

Aspects:
- Electronic Tech Logs (ETL), maintenance planning
- Remote diagnostics and aircraft data downloads

Elements:
- Tampering with maintenance records
- Compromise of predictive maintenance algorithms

Criteria:

- Digital signature and audit trails for task completion
- Security controls for BITE/aircraft data uploads
- Access control for ETL modification privileges

Security Services

Aspects:
- Screening systems (passenger and cargo)
- Surveillance systems (CCTV, intrusion detection)

Elements:
- Camera feed tampering or denial
- Spoofing of access credentials

Criteria:
- Continuous integrity monitoring
- Use of secure VPN and firewalled zones
- Logging of physical security access and overrides

Safety Management Systems (SMS)

Aspects:
- Safety data collection and analysis
- Confidential reporting systems

Elements:
- Risk of data exfiltration or manipulation
- Unauthorized access to safety occurrence reports

Criteria:
- Segregation of safety and operational data
- Encryption and anonymization of reporting tools
- Access reviews for safety databases

Operations Control / OCC

Aspects:
- Dispatch, crew scheduling, and disruption response
- Real-time fleet tracking and alerting

Elements:
- Delay propagation due to comms breakdown
- Compromise of crew rest/scheduling tools

Criteria:

- High-availability infrastructure
- Ransomware containment readiness
- Incident response simulations for OCC scenarios

General IT/Enterprise Services (cross-cutting domain)

Aspects:

- Email, intranet, HR and finance systems

Elements:

- Phishing, credential harvesting, financial fraud

Criteria:

- Phishing simulation and user awareness metrics
- Role-based access reviews for sensitive financial systems
- SOC (Security Operations Center) escalation protocols

Human Capital & Insider Threat Management

Aspects:

- Staff access to sensitive systems and data
- Employment lifecycle (recruitment → termination)
- Behavioral anomalies and trust-based exposures

Elements:

- Intentional sabotage, data theft, or system misuse
- Unintentional errors due to lack of awareness or fatigue
- Privilege misuse (e.g., system admins or maintenance certifiers)
- Social engineering or coercion by external actors

Criteria:

- **Pre-employment screening:**
  - Background and criminal checks for sensitive roles
  - Verification of professional qualifications and references

- **Access governance:**
  - Principle of least privilege (PoLP) enforced
  - Access rights reviewed at least quarterly or upon role change
  - Immediate revocation of access upon contract termination

- **Behavioral monitoring & anomaly detection:**

  - Implementation of User and Entity Behavior Analytics (UEBA)
  - Security alerts for abnormal access times or data transfers
  - Integration with safety or HR reporting mechanisms (e.g., stress, grievances)

- **Awareness and training:**
  - Cyber hygiene and data protection training upon induction and annually
  - Role-specific training for privileged users (e.g., IT admins, flight ops, maintenance planners)
  - Insider threat awareness sessions and simulated social engineering exercises

- **Psychosocial support and reporting mechanisms:**
  - Anonymous reporting channels for concerns (whistleblowing and behavioral anomalies)
  - Availability of mental health and employee assistance programs (EAP)
  - HR-Security-Safety coordination on performance or behavior concerns

- **HR & IT cooperation for employment lifecycle:**
  - Structured offboarding process to include exit interview and IT deprovisioning
  - Periodic reconciliation of employment and access lists
  - Secure destruction or retrieval of all issued hardware and credentials

- **Contractor and third-party access:**
  - Formal review and approval process for third-party access
  - Time-bound access control for temporary personnel
  - Mandatory cybersecurity awareness for all contract personnel

Reservations & Ticketing Systems

Aspects:
- Global Distribution Systems (GDS), Passenger Service Systems (PSS), and API integrations
- Payment processing and customer relationship management (CRM)
- Web-based booking portals and mobile applications

Elements:
- Exposure of PII, payment data, and itinerary information
- Unauthorized changes to bookings or manipulation of fare structures
- Fraudulent access or misuse of loyalty program accounts
- Availability risks (e.g., system outages, DDoS attacks)

Criteria:

- **Data Protection and Privacy Controls:**
  - Encryption of PII in transit and at rest (e.g., names, documents, email addresses, payment details)
  - Implementation of data minimization principles in line with GDPR and PCI-DSS
  - Data retention policy compliance and secure disposal of aged records

- **Authentication & Access Controls:**
  - Multi-factor authentication (MFA) for agent and staff portals
  - Secure customer login systems with CAPTCHA and brute-force protections
  - Session timeout and IP tracking for suspicious access attempts

- **Payment and Transaction Security:**
  - PCI-DSS compliance for all payment interfaces
  - Secure tokenization of card data and fraud detection rules in place
  - Alerts for unusual transaction volumes or patterns

- **Change Control and Booking Integrity:**
  - Audit trails for booking and ticket changes (manual and system-initiated)
  - Restrictions on override functions by supervisory levels only
  - Validation of third-party API requests (e.g., travel agents, consolidators)

- **Web & App Security:**
  - Regular penetration testing and OWASP Top 10 compliance for public portals
  - TLS/SSL encryption on all public-facing systems
  - Use of WAF (Web Application Firewall) and bot protection services

- **Fraud & Abuse Monitoring:**
  - Anomaly detection for loyalty points redemptions, cancellations, and refunds
  - Integration with fraud detection systems for known traveler patterns
  - Geolocation-aware login and access restrictions

- **Business Continuity & Incident Response:**
  - Backup and redundancy of reservation systems in secondary data centers or cloud
  - Runbooks for restoration of booking services during cyber incidents
  - Real-time dashboards for reservation flow and error trends