Security Department – Information Security Management System (ISMS) – Process Review Document

Governance & Context Establishment

Security Information Security Objectives: The Security Department's ISMS objectives are aligned with the organisation's safety, compliance, and operational continuity requirements. Objectives are reviewed annually and integrated into the wider organisational management system.

1. Protect the confidentiality, integrity, and availability (CIA) of physical and digital security information.
2. Prevent unauthorized access to secure areas, systems, and sensitive data.
3. Detect and respond effectively to physical and cyber security incidents.
4. Maintain compliance with applicable security regulations (e.g., EC 300/2008, EASA 2023/203, ICAO Annex 17).
5. Promote awareness and security competence across all roles.
6. Continuously improve the effectiveness and resilience of the security framework.

Expanded Security Information Security Objectives

The Security Department's ISMS objectives are designed to ensure the protection of people, assets, operations, and data in line with the organisation's safety, compliance, and business continuity goals. These objectives are subject to review during annual ISMS management reviews and are continually assessed for relevance in a changing threat landscape.

1. Protect the Confidentiality, Integrity, and Availability (CIA) of Physical and Digital Security Information

To maintain secure operations, both physical documents (e.g., access logs, visitor registers) and digital systems (e.g., CCTV storage, biometric access logs, threat databases) must be protected from unauthorized viewing, tampering, or loss.

Examples:

- Encrypted storage of video surveillance footage with retention policies.
- Controlled access to the security incident reporting system using multi-factor authentication (MFA).
- Use of tamper-evident seals on physical security documentation stored in lockable cabinets.

2. Prevent Unauthorized Access to Secure Areas, Systems, and Sensitive Data
This includes physical zones such as airside areas, cargo warehouses, and aircraft during turnaround, as well as digital systems like the electronic identity management system or airport perimeter sensor feeds.
Examples:

- Implementation of badge readers and facial recognition for airside access.
- Role-based access to cargo manifest systems to limit who can view or edit sensitive shipment data.
- Dual-authentication requirement for altering threat alert status within the security operations center (SOC).

3. Detect and Respond Effectively to Physical and Cyber Security Incidents
Incidents range from physical breaches (e.g., perimeter intrusion) to cyber threats (e.g., denial of service attack on access control servers). Effective detection, escalation, and coordinated response are critical to limit impact.
Examples:

- Use of AI-enabled behavior detection software at screening checkpoints to flag suspicious activity.
- Intrusion detection systems (IDS) monitoring for anomalous login attempts in the airport's digital security infrastructure.
- Structured emergency response drills simulating explosive threats or cyber-disruption of baggage tracking systems.

4. Maintain Compliance with Applicable Security Regulations
The ISMS ensures the Security Department remains compliant with legal and regulatory obligations, such as:

- **EU Regulation 300/2008** (common rules in the field of civil aviation security),
- **EASA Regulation 2023/203** (information security risk management),
- **ICAO Annex 17** (Safeguarding International Civil Aviation Against Acts of Unlawful Interference).

Examples:

- Maintaining audit trails to demonstrate compliance during ECAC or national authority inspections.
- Documented evidence of background checks, access revocations, and training records for all staff with unescorted access privileges.
- Reporting security incidents involving IT systems to the NIS authority as required under EU cybersecurity law.

5. Promote Awareness and Security Competence Across All Roles

A strong security culture depends on informed and vigilant personnel. The ISMS mandates role-based training and security briefings tailored to each function's responsibilities.

Examples:

- Security officers trained in behavioral threat recognition and non-invasive interrogation.
- Cybersecurity awareness for control room staff covering phishing attacks and secure data handling.
- Emergency scenario briefings for frontline staff at shift changes to reinforce readiness.

6. Continuously Improve the Effectiveness and Resilience of the Security Framework

Through systematic evaluation and feedback loops, the ISMS fosters a dynamic security posture that adapts to evolving threats, technology, and business operations.

Examples:

- Analysis of incident trends leading to upgrades in perimeter lighting and sensor calibration.
- Audit finding identifying outdated firmware on X-ray machines prompts fleet-wide update.
- Lessons learned from tabletop exercises lead to revised response checklists and better interdepartmental coordination protocols.

2. Scope of the ISMS

Organisational Context: This ISMS applies to the Security Department and covers all activities involved in protecting passengers, assets, infrastructure, and information from intentional and unintentional threats.

Departments and Business Areas Covered:

- Passenger Security
- Aircraft Security
- Facility Security
- Cargo Security
- Cybersecurity

- Employee Security
- Access Control
- Threat Assessment & Intelligence
- Emergency Response
- Compliance
- Training & Awareness

Scope of the ISMS – In-Depth Discussion

Organisational Context

The ISMS applies comprehensively to the **Security Department** of the organization, integrating both physical and digital security practices to ensure the protection of:

- **Passengers** – safeguarding personal safety and privacy;
- **Assets** – including aircraft, ground support equipment, IT systems;
- **Infrastructure** – terminals, hangars, fences, data centers, and control rooms;
- **Information** – operational data, personal data, incident logs, and surveillance records.

The ISMS encompasses both **intentional threats** (e.g., sabotage, cyberattacks, terrorism) and **unintentional threats** (e.g., human error, system failure, power outage) in a **prevention–detection–response–recovery** model.

Departments and Business Areas Covered

1. Passenger Security

Focuses on screening and safeguarding passengers throughout their journey, from curbside to boarding.

Examples:

- Use of walkthrough metal detectors (WTMD), X-ray screening, and explosive trace detection (ETD).
- Passenger behavior observation techniques to identify pre-incident indicators (e.g., evasiveness or erratic behavior).
- Secure management of personal identification data during the screening process.

2. Aircraft Security

Involves protection of the aircraft during ground time and ensuring its integrity before and after each flight.

Examples:

- Pre-departure aircraft searches for prohibited items or sabotage tools.
- Sealing of aircraft doors after security sweep and tagging of security-checked areas.

- Escort protocols for third-party maintenance or catering staff with controlled time-window access.

3. Facility Security
Covers both airside and landside infrastructure, including terminals, control rooms, and hangars.
Examples:

- Surveillance via CCTV and AI-enhanced motion detection in sterile zones.
- Controlled door access using RFID badges linked to biometric verification.
- Perimeter intrusion detection systems to detect breaches at fences or gates.

4. Cargo Security
Ensures integrity of inbound and outbound cargo and mail to prevent threats such as concealed explosives or smuggled contraband.
Examples:

- Mandatory cargo x-ray screening and seal verification on ULDs (Unit Load Devices).
- Chain-of-custody logging through RFID or GPS tagging from acceptance to loading.
- Enhanced screening procedures for cargo from high-risk regions or unknown consignors.

5. Cybersecurity
Protects the digital infrastructure that supports physical security systems and critical operations.
Examples:

- Firewall and intrusion detection system (IDS) monitoring on CCTV and badge server networks.
- Multifactor authentication (MFA) for access to control room applications and surveillance archives.
- Endpoint protection on mobile security team tablets used to log incident reports.

6. Employee Security
Manages background vetting, credentialing, and real-time monitoring of staff activities, especially those with unescorted access.
Examples:

- Pre-employment criminal and security checks aligned with regulatory requirements.
- Revocation of access rights within minutes of contract termination or job change.
- Investigation workflows for insider threat scenarios or behavioral red flags.

7. Access Control
Ensures that only authorized personnel can access secure areas, systems, or equipment.
Examples:

- Time-based access permissions preventing after-hours entry to high-security zones.
- Real-time logging and analytics of card swipe activity at airside doors.
- Dual-control entry procedures for control rooms or vaults (two-person authentication).

8. Threat Assessment & Intelligence
Focuses on gathering, evaluating, and acting on security-related intelligence in real time or preemptively.
Examples:

- Open-source intelligence (OSINT) monitoring of protest activity near airport premises.
- Participation in government-led threat intelligence briefings (e.g., from civil aviation authority or law enforcement).
- Dynamic threat level escalation protocols based on received alerts or observed patterns.

9. Emergency Response
Prepares for and coordinates actions in the event of a major security or safety incident.
Examples:

- Full-scale simulated hijacking exercise with joint response from law enforcement and airport staff.
- Emergency communication protocols via secured radio channels and mobile alerts.
- Activation of assembly zones and rapid lockdown capability in the event of terminal evacuation.

10. Compliance
Ensures all security activities meet international, regional, and national regulatory frameworks and standards.
Examples:

- Alignment with Regulation (EU) 300/2008 for passenger and baggage screening requirements.
- Integration of IS.I.OR. requirements for incident response, risk assessment, and continuous improvement.
- Audit readiness and evidence management for national authority security inspections.

11. Training & Awareness
Develops knowledge, competence, and vigilance in all roles through structured education and testing.
Examples:

- Induction training for new security officers with role-specific modules.
- Refresher courses on explosive detection recognition and emergency handling.
- Phishing awareness and secure data handling training for security control room personnel.

3. Roles & Responsibilities

- **Security Director**: Accountable for ISMS implementation and effectiveness.
- **Security Managers**: Oversee specific domains (e.g., airport, aircraft, cybersecurity).
- **Supervisors**: Ensure frontline compliance and support incident response.
- **Security Officers**: Execute operational duties in alignment with protocols.
- **Cybersecurity Specialists**: Secure systems and respond to digital threats.
- **Intelligence Analysts**: Monitor threats and feed assessments into planning.
- **Emergency Coordinators**: Lead incident response and drills.
- **Compliance Officers**: Monitor adherence to internal and external regulations.

4. Stakeholders & Interfaces

Internal Stakeholders:

- Airport Operations
- CAMO/Maintenance (aircraft access coordination)
- IT/Cybersecurity
- Emergency Response Team

Stakeholders & Interfaces – In-Depth Discussion
Effective security management in the aviation environment depends on close cooperation and continuous information flow between the Security Department and key

internal stakeholders. These relationships are essential for both **proactive threat mitigation** and **rapid response** to security incidents.

Internal Stakeholders

1. Airport Operations

Function:

Airport Operations (APOPS) is responsible for managing the day-to-day flow of aircraft, passengers, baggage, and ground handling services. This department directly interfaces with Security to ensure a seamless, safe operational environment.

ISMS Interface & Examples:

- **Queue Management at Screening Points:** Coordination to deploy additional security officers during peak traffic hours to prevent long queues that may create vulnerabilities.
- **Restricted Area Access Coordination:** Airport Ops oversees ramp and gate activities and must coordinate with Security for escorting unauthorized or temporary personnel (e.g., film crews, visiting technicians).
- **Terminal Incident Protocols:** If a suspicious package is detected, APOPS coordinates evacuation routes and passenger redirection while Security conducts the investigation.

Example Scenario:

During a power outage, Airport Operations activates backup generators while Security ensures CCTV, access control, and perimeter sensors remain functional. Both departments align through a joint continuity plan defined in the ISMS.

2. CAMO/Maintenance (Aircraft Access Coordination)

Function:

The Continuing Airworthiness Management Organisation (CAMO) and Maintenance teams ensure the technical airworthiness of the aircraft. They rely on controlled and timely access to aircraft for inspections, troubleshooting, and defect rectification.

ISMS Interface & Examples:

- **Controlled Aircraft Access:** Security verifies and logs all maintenance personnel entering airside or accessing parked aircraft. Any deviation (e.g., technician not listed on approved roster) triggers an access denial and security notification.
- **Work Order Timing and Escorting:** For late-night line maintenance, CAMO notifies Security in advance. Escorts may be required for non-credentialed vendors.
- **Data Sharing and System Integrity:** If CAMO uses tablets or mobile terminals to access technical data, Security ensures endpoint protection and audit logging of access sessions.

Example Scenario:

A night-shift maintenance technician is caught tailgating through a secure gate. Security

investigates the breach, and CAMO participates in a joint root cause review, followed by corrective actions including retraining and re-authorization.

3. IT/Cybersecurity

Function:

The IT/Cybersecurity unit safeguards the organization's digital infrastructure, from access control servers and surveillance storage to badge issuance systems and incident databases.

ISMS Interface & Examples:

- **System Hardening & Patch Management:** Security systems (e.g., biometric readers, badge printers, surveillance storage) are considered critical infrastructure. Cybersecurity ensures regular vulnerability scanning and patch updates.
- **Security Information and Event Management (SIEM):** Security events (e.g., repeated failed badge swipes or camera network disruptions) are logged centrally and monitored for real-time alerts.
- **Access Logs and Digital Forensics:** In case of suspected credential abuse or a badge cloning attempt, the Cybersecurity team assists in isolating logs, securing backups, and performing a forensic review.

Example Scenario:

A phishing email targets Security Control staff asking them to click a link to verify a camera feed. The Cybersecurity team investigates the email source, confirms whether any breach occurred, and implements spam filter updates while Security follows up with awareness reinforcement.

4. Emergency Response Team

Function:

The Emergency Response Team (ERT) leads the operational and tactical response to security, safety, or emergency events, including bomb threats, active threats, major accidents, or system failures.

ISMS Interface & Examples:

- **Joint Emergency Preparedness Exercises:** Security and ERT conduct coordinated drills, including terminal lockdown simulations or active shooter scenarios, with full communication plan rehearsals.
- **Alarm & Escalation Protocols:** A fire alarm or suspicious item triggers both ERT and Security responses. ERT handles medical/fire support while Security secures the perimeter and assists with crowd control.
- **Incident Post-Mortems and Lessons Learned:** After any event, ERT and Security jointly review what went well, what failed, and which ISMS procedures need updating.

Example Scenario:
During a suspicious package incident, Security initiates containment and alerts ERT. ERT contacts fire and police services, coordinates evacuation, and deploys first aid. A shared incident report is filed into the ISMS platform, with lessons integrated into future response protocols.

External Stakeholders:

- Law Enforcement
- National Aviation Authorities
- Third-party security providers
- Regulatory bodies (e.g., TSA, ICAO, EASA)

National Aviation Authorities - Role and Relevance to ISMS:
Authorities such as the Civil Aviation Authority (CAA) or equivalent oversee security standards enforcement, audit organizational compliance, and issue directives (e.g., security advisories, threat updates).
ISMS Considerations:

- Ensure procedures exist for responding to unannounced audits and submitting compliance evidence (e.g., access control logs, training records).
- Maintain access for regulators to securely review risk assessments, ISMS policies, and incident handling procedures.
- Participate in national security exercises and integrate lessons into security controls and response plans.

Example:
Following a regional airport breach, the national aviation authority issues a directive to increase random screening frequency and strengthen baggage handling controls. The Security Department updates its ISMS documentation, trains screening officers, and logs all updates for compliance verification.

Third-Party Security Providers - Role and Relevance to ISMS:
External service providers (e.g., contract screening officers, canine detection units, access control maintenance teams) operate within the security perimeter and often have access to critical systems or zones.
ISMS Considerations:

- Conduct vetting and onboarding procedures including background checks, non-disclosure agreements (NDAs), and security awareness briefings.
- Limit access to systems and areas strictly to defined job roles using time-bound permissions and badge management.
- Ensure contract clauses include ISMS-related obligations (e.g., incident reporting, system use protocols).

Example:
A third-party contractor servicing badge reader systems notices a configuration anomaly. Their SOP requires immediate reporting to the Security IT liaison. The anomaly is reviewed, and the action taken is documented in the ISMS change log. An internal audit is triggered to verify that other devices remain uncompromised.

Regulatory Bodies (e.g., TSA, ICAO, EASA) - Role and Relevance to ISMS:
These organizations establish international and regional frameworks for aviation security (e.g., ICAO Annex 17, EU Regulation 300/2008, EASA Regulation 2023/203). They set mandatory minimum standards and assess implementation effectiveness across member states.

ISMS Considerations:

- Regularly review and align internal policies with changes in external regulations (e.g., new EASA AMC/GM guidance).
- Maintain regulatory correspondence logs and version-controlled policy documentation to ensure traceability.
- Implement ISMS improvement cycles based on external audit outcomes or regulatory amendments.

Example:
EASA updates its guidance to require enhanced cybersecurity coordination between airport and aircraft systems. The Security Department, in coordination with Cybersecurity, updates its ISMS scope to include risk scenarios involving integrated airport-aircraft data flows (e.g., digital gate-to-cockpit messages), revises access protocols, and trains affected staff.

5. Asset Identification

Digital Assets:

- CCTV systems
- Access control systems
- Security incident logging systems

- Identity management databases
- Communication networks (radios, VoIP, encrypted email)

Asset Identification – Digital Assets in Detail
Digital assets are the core enablers of modern security operations. The ISMS mandates their **classification, ownership, protection**, and **auditability** based on their impact on the confidentiality, integrity, and availability (CIA) of security functions.

1. CCTV Systems
Purpose:
CCTV systems are deployed for real-time surveillance, deterrence, and forensic investigation of security incidents. They cover passenger terminals, aircraft parking areas, perimeter zones, and secure facilities.
ISMS Considerations:

- **Confidentiality:** Footage may contain sensitive images of individuals and must be protected from unauthorized access.
- **Integrity:** Tampering with or deletion of footage must be prevented.
- **Availability:** Cameras must be operational 24/7, with redundant storage (e.g., local DVR + cloud backup).

Examples:

- All footage is stored in an encrypted format and retained for a legally defined duration (e.g., 30–90 days).
- Audit logs track who accessed or exported any footage and when.
- Surveillance management consoles are isolated from the general network with two-factor authentication (2FA).

2. Access Control Systems
Purpose:
Digital access control systems manage, authorize, and log the entry and exit of individuals across various restricted zones using credentials like badges, PINs, or biometrics.
ISMS Considerations:

- **Confidentiality:** Badge data must be protected to prevent cloning or impersonation.
- **Integrity:** Logs of access must be tamper-proof and used as evidence in incident investigations.
- **Availability:** Systems must not fail in a way that allows unaudited access or causes unsafe egress lockouts.

Examples:

- Role-based access profiles ensure that staff can only access authorized areas.

- Time-bound access windows for contractors and vendors are automatically enforced.
- Alerting is triggered when badge attempts exceed defined failure thresholds (e.g., tailgating detection).

3.Security Incident Logging Systems
Purpose:
These systems record all reported security incidents, from suspicious behavior to physical breaches and cyber anomalies. They form the basis for investigation, trend analysis, and regulatory reporting.
ISMS Considerations:

- **Confidentiality:** Incident records often include personal data and must comply with data protection laws (e.g., GDPR).
- **Integrity:** Logs must be complete, timestamped, and unalterable.
- **Availability:** Investigators and management must be able to retrieve historical records during audits or legal processes.

Examples:

- Access to incident logs is restricted to designated roles and reviewed periodically.
- Every log entry includes metadata: who entered it, when, and what supporting documents (e.g., images, reports) are attached.
- Export functions are disabled for general users to prevent data leakage.

4. Identity Management Databases
Purpose:
These databases maintain personnel credentials, roles, vetting status, badge issuance history, and access permissions. They serve as the foundation for access control and accountability.
ISMS Considerations:

- **Confidentiality:** Contains personally identifiable information (PII) and security clearance levels.
- **Integrity:** Any changes to a person's access level must be logged and authorized.
- **Availability:** Must remain accessible to badge issuance centers and SOCs for real-time updates.

Examples:

- Integration with HR onboarding/offboarding workflows ensures automatic revocation of access when employment ends.
- Periodic reconciliation ensures inactive users are deactivated or archived.
- All actions on records (e.g., clearance level updates) require dual authorization and leave an audit trail.

5. Communication Networks (Radios, VoIP, Encrypted Email)

Purpose:
These systems ensure secure communication across security personnel, management, emergency responders, and external stakeholders.
ISMS Considerations:

- **Confidentiality:** Critical for preserving operational secrecy, especially during active incidents.
- **Integrity:** Messages must be transmitted as intended and without interference.
- **Availability:** Networks must function in emergencies, with failover and redundancy built in.

Examples:

- Use of AES-256 encrypted push-to-talk (PTT) radios on secured frequency bands.
- VoIP platforms configured with TLS encryption and access control restrictions for incident communication.
- Use of digital certificates for email signatures and encryption of sensitive messages (e.g., to regulators or law enforcement).

ISMS Protection Measures for Digital Assets
To safeguard these digital assets, the ISMS applies:

- **Asset classification schemes** (e.g., Critical / Confidential / Operational).
- **Ownership assignment** (e.g., CCTV system owned by Head of Surveillance).
- **Vulnerability assessments** and patching schedules.
- **Logging and audit mechanisms**.
- **Business continuity and disaster recovery (BC/DR)** planning.

Physical Assets:

- Screening equipment (X-ray, ETD, WTMD)
- Physical barriers (doors, gates, fences)
- Secure storage areas
- Emergency response equipment

Physical Assets in Information Security Management Systems (ISMS) – Issues, Requirements, and Examples
Inclusion of physical asset management within the ISMS ensures a holistic approach to security. Each asset must be documented, assigned an owner, and assessed for

vulnerabilities. Risk treatment plans should address maintenance, access control, incident response, and continuous monitoring. This layered defense supports the resilience of the aviation security ecosystem and aligns with EASA Regulation 2023/203 and ICAO Annex 17 best practices.

1. Screening Equipment (X-ray, ETD, WTMD)

Issues:

- Sensitivity calibration affects detection reliability.
- Physical tampering or unauthorized shutdown could compromise security.
- Equipment downtime creates operational bottlenecks.

Requirements:

- Regular maintenance and calibration per manufacturer and regulatory guidelines.
- Physical safeguards to prevent tampering or sabotage.
- Backup screening solutions (redundant units or rapid repair contracts).
- Access restriction to trained and certified operators only.

Examples:

- X-ray machines in baggage screening areas have tamper-evident seals and surveillance monitoring.
- Explosive Trace Detection (ETD) units have restricted access login and require two-person authentication for calibration adjustments.
- Walkthrough Metal Detectors (WTMDs) are tested daily using test objects, with failure logs stored for regulatory audit.

2. Physical Barriers (Doors, Gates, Fences)

Issues:

- Physical degradation or wear compromising barrier integrity.
- Unauthorized access due to manual override or lack of supervision.
- Vulnerabilities at access junctions (e.g., vehicle gates, emergency exits).

Requirements:

- Routine inspection protocols and maintenance schedules.
- Integration with access control systems (e.g., badge readers, biometrics).
- Intrusion detection alarms and real-time alerting to security control rooms.
- Emergency override capabilities documented and regularly tested.

Examples:

- Security gates to airside zones have badge and biometric readers backed by real-time surveillance.

- Fences are equipped with vibration sensors that trigger alarms on climbing or cutting.
- Access doors to the control room require dual-authentication and are logged through an audit trail system.

3. Secure Storage Areas

Issues:

- Inadequate locking mechanisms or poor access control.
- Storage of sensitive materials (e.g., confiscated items, secure documents) without audit mechanisms.
- Environmental risks such as fire, water damage, or humidity.

Requirements:

- Secure, fire-resistant, and access-controlled facilities.
- Electronic logging of all access events.
- Environmental controls (e.g., temperature, humidity, smoke detectors).
- Clearly defined retention, disposal, and access policies.

Examples:

- A secure locker room for weapons and restricted items with access granted only to armed guards and supervisors.
- Document safes storing incident logs are fire-rated and monitored via internal CCTV.
- Storage areas for biometric enrolment kits are alarmed and accessed through controlled keycard entry only.

4. Emergency Response Equipment

Issues:

- Poorly maintained or expired emergency supplies (e.g., fire extinguishers, first aid kits).
- Lack of staff familiarity with emergency equipment locations and usage.
- Equipment not suited for current operational threats (e.g., missing chemical spill kits in cargo areas).

Requirements:

- Inventory checks and maintenance logs for all emergency equipment.
- Accessibility in line with emergency evacuation maps and protocols.
- Regular staff training and drills to ensure readiness.
- Review of adequacy based on evolving threat assessments.

6. Risk Assessment

Risks are assessed in accordance with IS.I.OR.205 and include:

- Insider threats
- Unauthorized access
- Cyber intrusion into security systems
- Sabotage or tampering of aircraft or cargo
- Failure of screening technologies

ISMS Risk Assessment – Aviation Security Department
Under the guidance of IS.I.OR.205, the Security Department implements a structured risk assessment process to identify, evaluate, and mitigate risks to physical, digital, and operational assets. These risks are evaluated based on potential impact, likelihood, and control effectiveness, and feed directly into the organisation's risk treatment and continuous improvement strategy.
Key Risk Areas and Examples

1. Insider Threats
Definition: Risks posed by individuals with authorized access (e.g., employees, contractors) who may intentionally or inadvertently compromise security.
Examples:
- A security guard disabling a CCTV camera before committing theft.
- A technician leaking sensitive access credentials to unauthorized personnel.

ISMS Approach:
- Mandatory background checks and continuous vetting.
- Role-based access control and logging.
- Whistleblower protections and anonymous reporting channels.

2. Unauthorized Access
Definition: Entry into restricted or secure areas by individuals without appropriate authorization.
Examples:
- An individual using a cloned ID badge to enter a restricted cargo area.
- A tailgating incident where an intruder follows a staff member into a secure zone.

ISMS Approach:

- Deployment of biometric and multi-factor authentication at high-risk access points.
- Installation of anti-tailgating turnstiles and motion sensors.
- Real-time monitoring and automated alerting via access logs and surveillance systems.

3. Cyber Intrusion into Security Systems
Definition: Digital attacks targeting infrastructure that supports physical security, such as surveillance, access control, or communication systems.
Examples:

- Malware introduced via a phishing email that disables the access badge database.
- Remote hacking into airport perimeter alarm systems.

ISMS Approach:

- Network segmentation and zero-trust architecture for all critical systems.
- Real-time intrusion detection systems (IDS) and threat hunting.
- Regular penetration testing and cybersecurity drills involving the SOC.

4. Sabotage or Tampering of Aircraft or Cargo
Definition: Deliberate interference with aircraft, cargo, or supporting infrastructure to cause damage, delay, or harm.
Examples:

- Intentional tampering with aircraft wiring while on the ground.
- Concealment of dangerous goods within high-value cargo.

ISMS Approach:

- Tamper-evident seals and chain-of-custody protocols for aircraft and cargo.
- Surveillance and security patrols of critical apron and hangar areas.
- Threat assessments on high-risk shipments and randomised cargo checks.

5. Failure of Screening Technologies
Definition: Malfunction or misconfiguration of equipment used to detect threats (e.g., explosives, weapons, prohibited items).
Examples:

- Explosive Trace Detection (ETD) unit failure during peak operations.
- Walkthrough Metal Detectors (WTMD) failing to detect test objects due to calibration drift.

ISMS Approach:

- Daily pre-use testing and logging for all screening equipment.
- Scheduled calibration and third-party maintenance.
- Equipment redundancy and failover plans to prevent checkpoint delays.

7. Controls Implementation

Controls are mapped to identified risks and include:

- Biometric and badge-based access control
- Red teaming and penetration testing
- Firewalls, intrusion detection systems (IDS)
- Secure procedures for cargo/baggage handling
- Role-based permissions and audit trails

7. Controls Implementation – Aviation Security ISMS

Control implementation is the operational backbone of the ISMS. Each control must be justified through risk linkage, assessed for cost-effectiveness, and monitored for efficacy. Together, these controls form a multi-layered defense posture that protects aviation security environments from emerging threats while fulfilling regulatory and organizational mandates.

Following the identification and assessment of risks under IS.I.OR.205, the implementation of security controls becomes essential to mitigate threats, enforce compliance, and strengthen resilience. The selected controls must be appropriate to the nature of the threat, tailored to operational realities, and continuously evaluated for effectiveness.

Control Areas and Examples

1. Biometric and Badge-Based Access Control

Purpose: To ensure that only authorized personnel can access sensitive areas and systems.

Examples of Use:

- Biometric fingerprint readers at airside access points.
- Dual authentication (badge and biometric) required for control room entry.
- Deactivation of badges upon contract termination or reassignment.

ISMS Role:

- Mitigates insider threats and unauthorized access.
- Integrates with audit logging to support investigations.
- Supports compliance with access control requirements of EASA and ICAO Annex 17.

2. Red Teaming and Penetration Testing

Purpose: To simulate real-world adversarial behavior and evaluate security resilience.

Examples of Use:

- Scheduled red team exercises to test perimeter security and response readiness.
- Social engineering simulations targeting staff to assess phishing awareness.
- Penetration tests on badge control systems and security infrastructure.

ISMS Role:

- Identifies hidden vulnerabilities before they can be exploited.
- Provides data-driven insights for control improvement.
- Ensures system robustness under simulated threat conditions.

3. Firewalls and Intrusion Detection Systems (IDS)

Purpose: To prevent, detect, and alert against unauthorized digital access to security-critical systems.

Examples of Use:

- Firewall rules restricting internet access to the access control database.
- IDS tools monitoring for anomalies in badge login activity or camera feeds.
- Email filtering systems identifying malware-laced security advisories.

ISMS Role:

- Safeguards against cyber intrusions targeting physical security systems.
- Enables log correlation and threat hunting across network and application layers.
- Fulfills cybersecurity oversight under Regulation (EU) 2023/203.

4. Secure Procedures for Cargo/Baggage Handling

Purpose: To prevent unauthorized tampering, theft, or introduction of prohibited items in cargo and baggage workflows.

Examples of Use:

- Chain-of-custody tracking for high-risk cargo items.
- CCTV coverage of all baggage handling touchpoints.
- Real-time reconciliation of baggage counts and declared manifests.

ISMS Role:

- Mitigates risks of sabotage and loss of critical goods.
- Enables auditing of handling procedures for security compliance.
- Aligns with EU Regulation 300/2008 and ICAO Annex 17 provisions.

5. Role-Based Permissions and Audit Trails

Purpose: To ensure staff access is limited to the minimum required for job function, and that all actions are traceable.

Examples of Use:

- Only certified security officers can operate or calibrate screening equipment.
- Access to surveillance logs is restricted to senior supervisors.
- All login attempts and system changes are automatically logged.

ISMS Role:

- Reduces exposure from insider threats.
- Supports forensic analysis and post-incident review.
- Enables compliance with traceability and accountability obligations.

8. Incident Detection, Response & Recovery

Follow IS.I.OR.220 framework:

- Define incident severity and escalation levels
- Establish reporting workflows
- Implement containment and recovery plans
- Maintain incident logs and conduct post-mortem analysis

8. Incident Detection, Response & Recovery – Aviation Security ISMS

Incident handling is a critical component of an Information Security Management System (ISMS). In accordance with IS.I.OR.220, a structured approach is required to ensure timely detection, effective response, and full recovery from security-related incidents. This section defines the framework and provides operational examples.

1. Define Incident Severity and Escalation Levels

Purpose: Classify incidents based on potential or actual impact to prioritize resource allocation and escalation protocols.

Severity Levels:

- **Level 1 (Low):** Minor equipment malfunctions with no security breach.
- **Level 2 (Moderate):** Attempted unauthorized access with no confirmed breach.
- **Level 3 (High):** Confirmed breach of security perimeter or IT system.
- **Level 4 (Critical):** Ongoing or successful coordinated attack, e.g., sabotage, hijacking, or cyberattack.

Example:

- A badge cloning attempt is detected—escalated from Level 2 to Level 3 after correlation with unauthorized door access and system alerts.

2. Establish Reporting Workflows

Purpose: Enable rapid reporting and validation of potential security incidents through predefined channels.

Process:

- All staff must report suspected incidents immediately via internal security hotline or system.
- Security Control Centre (SCC) logs initial reports, triggers triage.
- Duty Supervisor validates incident and notifies relevant teams (e.g., cybersecurity, emergency response).

Example:

- A security officer discovers signs of tampering on the cargo fence. The officer alerts SCC, which activates the perimeter incident protocol and notifies surveillance and operations.

3. Implement Containment and Recovery Plans

Purpose: Prevent further damage and restore secure operations promptly.

Containment Actions:

- Isolate affected systems or areas.
- Revoke access credentials.
- Deploy on-site security or cyber incident teams.

Recovery Actions:

- Replace or repair affected assets.
- Reset system credentials and reconfigure affected IT systems.
- Resume operations following validation.

Example:

- During a cyber intrusion into the access control network, containment includes network isolation and firewall rule adjustment. Recovery includes system audit, patch deployment, and account restoration.

4. Maintain Incident Logs and Conduct Post-Mortem Analysis

Purpose: Ensure transparency, accountability, and continuous improvement.

Requirements:

- Log all incidents, actions taken, and recovery outcomes.
- Conduct a root cause analysis within 48–72 hours of closure.
- Document lessons learned and implement changes to controls or policies.

Example:

- After an insider breach at a secure baggage screening area, a full post-mortem reveals a breakdown in supervisor sign-off procedures. As a result, procedures are updated, and additional training is introduced.

Conclusion

A disciplined approach to incident detection, response, and recovery strengthens the ISMS by limiting impact, restoring trust, and improving future resilience. Aligning practices with IS.I.OR.220 ensures that all aviation security incidents—whether physical or digital—are managed within a mature, auditable, and compliant framework.

9. Compliance & Audit

Regular internal audits assess:

- Conformance to Regulation (EU) 2023/203 and other applicable standards
- Effectiveness of controls
- Training and awareness levels
- Incident trends and responses

9. Compliance & Audit – Aviation Security ISMS

An effective ISMS relies on robust compliance verification and structured auditing processes. In line with the principles outlined in Regulation (EU) 2023/203 and IS.I.OR.225, both internal departmental Quality Control (QC) and independent Quality Assurance (QA) play essential roles.

A dual-layered compliance and audit model, with QC embedded within departments and QA independently reviewing across the system, ensures continuous alignment with evolving regulatory expectations. Regular audits not only measure compliance but also drive accountability, reinforce security culture, and improve overall ISMS resilience.

Distinguishing QC and QA Responsibilities

- **Quality Control (QC):** Department-led oversight focusing on daily operational conformance. It ensures procedures are followed, systems are functional, and risks are managed.
- **Quality Assurance (QA):** Independent audit activities conducted by the compliance function or external parties to verify the effectiveness of the ISMS and the organisation's regulatory alignment.

1. Conformance to Regulation (EU) 2023/203 and Other Standards

QC Application:

- Routine checks on access control logs and alarm system responses.
- Security supervisors verify staff compliance with biometric access protocols.

QA Example:

- Quarterly audit to confirm ISMS documentation reflects the current version of Regulation 2023/203.
- Gap analysis between ICAO Annex 17 provisions and internal operating procedures.

2. Effectiveness of Controls

QC Application:

- Regular testing of screening equipment (e.g., ETD calibration, X-ray image quality).
- Supervisory review of badge deactivation logs and CCTV functionality.

QA Example:

- Independent evaluation of how access control failures are escalated and resolved.
- Penetration testing reports reviewed against red team drill outcomes.

3. Training and Awareness Levels

QC Application:

- Department heads verify attendance and test scores for mandatory security training.
- Security officers complete scenario-based refreshers every quarter.

QA Example:

- Annual audit of training matrix, including assessment of compliance with role-specific awareness requirements.
- Spot interviews conducted by QA to gauge frontline staff understanding of incident escalation.

4. Incident Trends and Responses

QC Application:

- Weekly review of incident logs to detect patterns or repeat offenses.
- Duty supervisors follow up on corrective actions for each incident.

QA Example:

- Biannual audit of the incident response framework: timeliness, containment measures, recovery validation.
- Post-incident reviews randomly selected for deep-dive analysis by the compliance team.

Achieving Compliance

- **Integrated Management System:** Embed ISMS checks into the broader operational and safety oversight cycle.

- **Document Control:** Ensure policies and records are version-controlled and accessible.
- **Audit Trail:** Maintain comprehensive audit logs for physical and digital activities.
- **Corrective Action Tracking:** Implement CAPA (Corrective and Preventive Action) for each QA finding.

Example:

- A QA audit discovers a lag in access revocation after staff termination. The compliance team issues a corrective action plan, updates HR-security coordination procedures, and sets a 30-day effectiveness review.

10. Training & Awareness

Training programs are delivered per domain and job role. Topics include:

- Threat recognition
- Use of security technology
- Emergency procedures
- Cyber hygiene

Training & Awareness – Aviation Security ISMS

Effective training and awareness are central to ensuring that all personnel understand and can execute their responsibilities within the Information Security Management System (ISMS). Training must be risk-informed, role-specific, and reviewed regularly to address emerging threats and evolving technologies.

By tailoring training to specific threats and responsibilities, and embedding a culture of security awareness, the ISMS builds resilience and compliance across the organization. Continuous learning, paired with practical reinforcement and leadership engagement, ensures that all personnel contribute to maintaining a secure aviation environment.

Training Program Structure

Training is structured by both domain (e.g., cyber, cargo, access control) and job role (e.g., security officer, supervisor, emergency response coordinator). Each employee receives baseline awareness training and then participates in specialized modules aligned with their duties and access level.

Key Training Topics and Examples

1. Threat Recognition
Purpose: Equip personnel to detect suspicious behavior, potential security breaches, or early signs of insider threats.
Examples:
- Security staff trained to identify behavioral indicators of surveillance or dry runs.
- Cargo handlers briefed on red flags in shipping documentation that could indicate smuggling or concealment of contraband.
- Access control personnel taught to recognize badge cloning techniques and tailgating attempts.

Delivery Methods:
- Classroom instruction, role-play scenarios, video-based learning.
- Regular briefings on recent threat intelligence and case studies.

2. Use of Security Technology
Purpose: Ensure proper use, configuration, and interpretation of technical tools such as screening systems, surveillance equipment, and access control infrastructure.
Examples:
- X-ray operators undergo certification training and image interpretation proficiency checks.
- Security supervisors receive refresher courses on managing biometric entry systems.
- IT and security integration teams trained to manage alert dashboards and video analytics software.

Delivery Methods:
- Vendor-led instruction, simulator-based training, and hands-on walkthroughs.
- Annual proficiency exams and recalibration workshops.

3. Emergency Procedures
Purpose: Prepare staff to respond effectively to security incidents such as fire, active threats, bomb threats, or cyberattacks.
Examples:
- Evacuation drills including scenario-based simulations.
- Cargo screening staff trained to handle suspicious package procedures.
- Supervisors trained in incident command and inter-agency coordination.

Delivery Methods:
- Emergency response drills, tabletop exercises, on-site walkthroughs.
- Team debriefings and after-action reviews (AARs).

4. Cyber Hygiene
Purpose: Promote digital awareness and reduce vulnerabilities linked to poor user behavior or lack of technical understanding.

Examples:

- Password management training and phishing simulation exercises.
- Guidance on secure use of personal and company devices.
- Data handling and secure communication protocols for mobile staff.

Delivery Methods:

- Online learning modules with interactive quizzes.
- Monthly tips and reminders through internal communication platforms.

Supporting Measures

- **Training Matrix:** A centralised database aligns training requirements with each position and monitors completion status.
- **Refresher Cycles:** Training is renewed annually or following any significant policy change or incident.
- **Competency Assessment:** Post-training assessments evaluate understanding and performance readiness.

11. Continuous Improvement

The ISMS is subject to periodic review, with:

- Key Performance Indicators (KPIs) monitored
- Lessons learned from incidents
- Recommendations from audits integrated
- Security roadmap updated annually

11. Continuous Improvement – Aviation Security ISMS

The principle of continuous improvement is fundamental to an effective Information Security Management System (ISMS). It ensures that security controls, processes, and organizational culture evolve in response to emerging threats, operational changes, and regulatory developments. Under the ISMS framework, continuous improvement is driven through structured reviews, performance monitoring, and strategic planning.

Continuous improvement transforms the ISMS from a static compliance mechanism into a living system that adapts, learns, and evolves. By integrating lessons learned, tracking KPIs, responding to audit outcomes, and maintaining a strategic roadmap, aviation security stakeholders ensure ongoing effectiveness, resilience, and regulatory compliance.

1. Key Performance Indicators (KPIs) Monitored

Purpose: Quantitative measurement of ISMS performance and security effectiveness across departments.

Examples of Security KPIs:

- Number of unauthorized access attempts blocked.
- Percentage of staff with up-to-date security training.
- Incident response time (detection to containment).
- Percentage of audit findings closed within target timeframe.

Guidance:

- Define measurable, realistic KPIs aligned with security objectives.
- Review KPIs monthly at departmental level and quarterly at ISMS Steering Committee level.
- Integrate KPIs into the broader corporate dashboard for visibility.

2. Lessons Learned from Incidents

Purpose: Use real-world events to improve detection, response, and prevention capabilities.

Examples:

- Following a phishing incident, staff training was revised to include advanced social engineering tactics.
- After a cargo tampering attempt, additional CCTV coverage and seal verification procedures were introduced.

Guidance:

- Conduct a post-incident review for all events classified as Severity Level 2 or higher.
- Document root causes, contributing factors, and remedial actions.
- Distribute lessons learned across all relevant departments and update related procedures.

3. Recommendations from Audits Integrated

Purpose: Ensure audit findings and external recommendations lead to tangible improvement.

Examples:

- An audit revealed inconsistent revocation of access credentials. The HR–Security interface was revised to mandate same-day revocation.
- Compliance audit highlighted outdated emergency response documentation, triggering a revision and reissuance cycle.

Guidance:

- Maintain an audit action tracker with clear responsibilities and deadlines.
- Review implementation effectiveness within 30 to 60 days of corrective action.
- Escalate non-closed findings to the ISMS Steering Committee.

4. Security Roadmap Updated Annually
Purpose: Strategically align security initiatives with long-term organizational goals.
Examples of Roadmap Elements:

- Implementation of AI-based behavior analytics for perimeter intrusion.
- Upgrade of screening equipment to meet new ECAC standards.
- Phased rollout of integrated physical-cyber incident management platform.

Guidance:

- Conduct an annual ISMS management review involving key stakeholders.
- Update roadmap based on performance data, risk landscape, audit outcomes, and regulatory changes.
- Communicate updates across departments to ensure transparency and alignment.

Building the Risk Register - consider the following risks as candidates for inclusion in the Risk Register

Governance & Systemic Risks

1. **ISMS Policy Misalignment** – ISMS objectives not aligned with organizational security strategy leading to inconsistent implementation.
2. **Incomplete Asset Inventory** – Unidentified or unclassified digital/physical assets expose the system to unmanaged vulnerabilities.
3. **Lack of Role-Based Accountability** – Undefined responsibilities across Security, CAMO, APOPS, or Cybersecurity cause delayed responses or control failures.

Insider Threat & Human Factors

4. **Malicious Insider Activity** – Credentialed personnel misusing access for sabotage, data leakage, or theft.
5. **Negligent Insider Exposure** – Staff unintentionally exposing credentials, misconfiguring systems, or failing to report anomalies.

6. **Unauthorized Information Disclosure** – Internal sharing of restricted intelligence or surveillance data violating CIA principles.
7. **Tailgating & Social Engineering** – Intruders bypassing access control by exploiting trust or tailing staff through secure doors.
8. **Training Deficiency** – Inadequate understanding of cyber hygiene, technology use, or incident response procedures.

Physical Security Risks

9. **Perimeter Breach** – Unauthorized entry via fence breach, gate compromise, or unmonitored emergency exits.
10. **Control Room Intrusion** – Unauthorized access to security operations centers due to badge cloning or poor monitoring.
11. **Tampering with Screening Equipment** – Disabling or altering the sensitivity of X-ray or ETD equipment.
12. **Compromised Storage Areas** – Unauthorized access to secure evidence rooms or document archives.
13. **Failure of Surveillance Systems** – Downtime or data loss in CCTV coverage due to hardware failure or power outages.
14. **Bypassed Biometric Controls** – System override, spoofing, or software vulnerabilities exploited to bypass biometrics.

Cybersecurity Risks

15. **Credential Theft via Phishing** – Social engineering or malicious links used to capture login credentials.
16. **Access Control System Breach** – Unauthorized digital access to badge database or reader configuration.
17. **Malware in Surveillance Network** – Malware impacting CCTV storage, feed integrity, or control software.

18. **Denial of Service (DoS) on Access Systems** – System overload affecting badge swipe validation and area lockdowns.
19. **Unauthorized Wireless Access** – Rogue devices gaining access through unsecured wireless or BYOD policies.
20. **Data Integrity Compromise** – Alteration or deletion of logs in security incident systems or identity databases.

Operational Interface Risks

21. **Uncontrolled Third-Party Access** – Contractors or vendors accessing restricted areas without escort or proper credentialing.
22. **Delayed Revocation of Access** – Ex-employees or reassigned staff retaining valid credentials.
23. **Unsecured Mobile Devices** – Tablets or smartphones used by security officers being compromised or lost.
24. **Lack of Joint Protocols with CAMO/APOPS** – Misalignment or communication breakdown during aircraft access or emergency response.
25. **Unlogged Emergency Access** – Bypassing normal controls during an emergency without post-access audit trail.

Cargo & Baggage Handling Risks

26. **Cargo Tampering or Substitution** – Unauthorized items placed in ULDs or manifest substitution.
27. **Failure of Chain-of-Custody** – Break in RFID/GPS tracking, leading to loss of location traceability.
28. **Misuse of Screening Exceptions** – Abuse of high-trust channels for fast-track cargo or baggage, bypassing screening.
29. **Lack of Enhanced Checks for High-Risk Cargo** – Inadequate profiling of origin or consignor history.

Incident Management & Response Risks

30. **Delayed Incident Reporting** – Frontline staff unaware or hesitant to report anomalies.
31. **Incomplete Incident Logs** – Missing evidence or unstructured documentation reducing investigative effectiveness.
32. **Inadequate Severity Classification** – Underestimating impact leading to poor escalation and resource allocation.
33. **Recovery Plan Failures** – Poor testing of backup systems or unclear recovery protocols during access control failure.

Compliance & Strategic Risks

34. **Non-Conformance with EU 2023/203 or ICAO Annex 17** – Gaps identified during audit inspections or external reviews.
35. **Failure to Act on Audit Findings** – Repeated or unmitigated risks due to ineffective corrective action programs.