Enterprise Information and Cyber Security in Relation to Business Continuity Planning (BCP) compliant with EASA Part IS

Introduction This document establishes the integrated framework for addressing information and cyber security as a key enabler of Business Continuity Planning (BCP) across multiple functional domains including operations, maintenance, ground handling, customer service, and administration.

The scope aligns with EU Regulation 2023/203 and 2022/1645, and supports enterprise-wide continuity, safety, and regulatory compliance.

Governance and Strategic BCP Integration The governance structure integrates BCP within the enterprise Information Security Management System (ISMS), under the direction of the Chief Information Security Officer (CISO), with active representation from all business units. The structure includes:

- **Board Oversight and Executive Responsibility:** Strategic BCP ownership rests with the executive board with direct accountability assigned to the Chief Operating Officer and CISO.
- **ISMS–BCP Governance Committee:** Cross-functional committee ensures coordination between security, operational resilience, compliance, and business units.
- **Policy Integration:** Unified enterprise ISMS and BCP policies mandate continuity and recovery standards across all departments.

Effective BCP governance must go beyond administrative coordination and embed cyber-resilience at the strategic, operational, and technical layers of the enterprise. Proactively identifying exposures within governance structures enables a more resilient and response-capable airline ecosystem.

- **Board Oversight and Executive Responsibility**
- **Function:** The executive board defines strategic risk tolerance, approves BCP investment priorities, and holds accountability for business resilience.
- **Cyber Exposure:**
- **Delayed Executive Awareness:** If C-suite is unaware of real-time cyber threats (e.g., spear-phishing of executive mailboxes), they may approve ineffective or outdated BCP strategies.
    - *Example:* A board member's account is compromised during a ransomware event; attacker uses access to delay response decisions or disable endpoint protection tools.

- **Shadow IT in Strategic Functions:** Executives using unsecured mobile apps or personal devices for critical communication may bypass corporate controls.
    - *Example:* The COO accesses real-time OCC dashboards via a non-compliant personal tablet during a major disruption, exposing operations data.
- **3. ISMS–BCP Governance Committee**
-
- **Function:** A cross-functional team tasked with overseeing the integration of BCP and ISMS across departments including IT, operations, compliance, safety, and HR.
- **Cyber Exposure:**
- **Poor Visibility across Domains:** Lack of integrated monitoring may prevent detection of lateral threat movement.
    - *Example:* Malware spreads from compromised vendor portal into HR systems unnoticed due to segmented risk assessments.
- **Cross-Domain Communication Breakdown:** Inadequate cyber-secure collaboration tools could hamper coordination during incidents.
    - *Example:* During a simulated BCP test, key stakeholders are unable to securely share logs or response plans due to expired digital certificates on shared platforms.
- **Fragmented Incident Playbooks:** Varying incident response maturity across departments leads to inconsistent recovery times and data loss.
    - *Example:* Maintenance department executes outdated BCP playbook, delaying restoration of AMOS data after attack.
- **4. Policy Integration Across the Enterprise**
- **Function:** Unified policies align continuity, cybersecurity, and regulatory compliance, providing a single reference for recovery standards and responsibilities.
- **Cyber Exposure:**
- **Policy Drift Between Departments:** Departmental deviations or delayed policy adoption create gaps in security enforcement.
    - *Example:* Ground-Handling team follows legacy data retention policy, leaving unencrypted USB backups in circulation.
- **Ineffective Control Mapping:** BCP controls not clearly mapped to cyber threats.
    - *Example:* PSS recovery policy focuses only on availability, not integrity, allowing replay attacks post-restoration.
- **Unaligned Vendor Controls:** Third-party vendors may lack enforcement mechanisms tied to enterprise BCP–ISMS alignment.
    - *Example:* CRM vendor hosting loyalty data fails to meet updated encryption standards, resulting in breach during a DDoS diversion event.

- **5. Recommendations for Strengthening Governance-Based Cyber Resilience**
- Formalise cyber threat intelligence briefings at board level.
- Ensure governance committee includes technical cyber expertise and decision-making authority.
- Mandate annual policy harmonisation audits across departments.
- Extend policy enforcement to third party SLAs with embedded cybersecurity KPIs.
- Use enterprise-wide BCP simulations to test governance coordination and cyber playbook accuracy.

Enterprise Risk and Continuity Objectives The organisation applies a risk-based BCP framework to ensure the Confidentiality, Integrity, and Availability (CIA) of critical information assets and services. Continuity objectives include:

- Maintain flight operations and dispatch services
- Preserve integrity of airworthiness and maintenance systems
- Sustain customer service, ticketing, and CRM platforms
- Ensure continuity of safety-critical communications and data flows

Enterprise Risk and Continuity Objectives – Detailed Assessment and Exposure Analysis

The continuity of enterprise aviation services depends on proactive risk identification, layered resilience controls, and aligned governance. This assessment forms the foundation for targeted mitigation strategies embedded within a holistic ISMS–BCP approach.

1. Introduction This document presents a detailed assessment of the enterprise risk and continuity objectives applied within the framework of a risk-based Business Continuity Planning (BCP) strategy. The overarching goal is to ensure the Confidentiality, Integrity, and Availability (CIA) of critical systems and data across the airline's core operational and support functions. The following sections analyse continuity objectives, outline associated cyber and operational exposures, and propose mitigation insights.

2. Maintain Flight Operations and Dispatch Services
Objective: Ensure uninterrupted functioning of the Operations Control Centre (OCC), flight dispatch platforms, crew rostering systems, and flight planning tools.

Key Systems:

- **Flight planning software (LIDO, Jeppesen)**
- **Crew management and rostering platforms**
- **EFB data delivery systems**
- **Flight tracking and NOTAM distribution portals**

Potential Exposures:

- **Cyberattack on OCC Infrastructure: Targeted malware disables dispatch servers, halting all aircraft release.**
  - ***Example:* Coordinated ransomware encrypts flight-planning servers, delaying multiple departures across hubs.**
- **Loss of Real-Time Communication: VPN failure prevents dispatchers from accessing integrated airspace data.**
  - ***Example:* OCC loses sync with ATC platforms during a connectivity fault, leading to emergency rerouting.**
- **Data Integrity Failure in Crew Rostering: Compromised schedule leads to insufficient rest or duplication errors.**
  - ***Example:* A logic injection corrupts crew assignment, triggering regulatory non-compliance.**

3. Preserve Integrity of Airworthiness and Maintenance Systems

Objective: Safeguard the digital backbone of the continuing airworthiness process, ensuring traceability and compliance.

Key Systems:

- **Maintenance management software (AMOS, TRAX, OASES)**
- **Technical log systems and component tracking**
- **Reliability analysis tools**
- **ARC issuance workflows**

Potential Exposures:

- **Corrupted Aircraft Status Data: Malware modifies deferred defect logs, concealing unaddressed critical items.**
  - ***Example:* Altered MEL/CDL entries result in unauthorized dispatch of a non-airworthy aircraft.**
- **Downtime during Heavy Check: AMO unable to retrieve maintenance plans due to system outage.**
  - ***Example:* Planned C-check halted due to corrupted task card database.**
- **Data Loss in ARC Generation: Archive breach deletes compliance evidence required for ARC renewal.**
  - ***Example:* Local server crash and insufficient backup lead to missed ARC deadlines for three aircraft.**

4. Sustain Customer Service, Ticketing, and CRM Platforms

Objective: Maintain passenger-facing digital infrastructure and protect sensitive customer and loyalty program data.
Key Systems:

- **Passenger Service System (PSS)**
- **Departure control system (DCS)**
- **Customer relationship management (CRM)**
- **Online check-in, booking, and mobile app services**

Potential Exposures:

- **DDoS Attack on Booking Engines: Public-facing portals crash during peak load.**
  - ***Example:* 12-hour booking blackout during holiday season causes reputational damage and revenue loss.**
- **Customer Data Breach via CRM Exploit: Threat actor exfiltrates loyalty points, emails, and payment tokens.**
  - ***Example:* Zero-day vulnerability in CRM exploited via compromised vendor integration.**
- **Ticketing Service Provider Downtime: Third-party outage cascades to check-in system failure.**
  - ***Example:* Inability to access DCS halts boarding for all flights out of a major hub.**

5. Ensure Continuity of Safety-Critical Communications and Data Flows
Objective: Guarantee availability and resilience of safety-sensitive communications (e.g., flight safety reports, operational messages, pilot/crew status).
Key Systems:

- **Crew communication and briefing platforms**
- **SMS and safety occurrence reporting tools**
- **Aircraft telemetry and ACARS messaging**
- **Security alert distribution channels**

Potential Exposures:

- **Delayed Safety Alerts: Failure in SMS system prevents escalation of in-flight hazard reports.**
  - ***Example:* Repetitive brake overheat issue goes unreported due to backend messaging queue fault.**
- **ACARS Tampering or Signal Loss: Aircraft telemetry disrupted during critical flight phase.**
  - ***Example:* Flight data falsified en route via compromised onboard comm module.**
- **Access Denial to Emergency Coordination Tools: Lockout from ERP during simultaneous multi-airport disruption.**
  - ***Example:* Dual outage at primary and backup sites disables crisis dashboard during weather-related diversion.**

6. Summary and Recommendations

- **Perform scenario-based testing for all critical systems under cyber-disruption and physical failure.**
- **Conduct control effectiveness mapping between ISMS and BCP domains.**
- **Enforce tighter monitoring of third-party platform integrity and backup resilience.**
- **Establish offline operational continuity procedures for OCC, ARC, and CRM functions.**

Major Enterprise Exposures:

- Coordinated ransomware attacks on operational systems (EFB, OCC, DCS)
- Data corruption in ERP affecting maintenance, logistics, and payroll
- Communication outages between dispatch and ATC or airports
- Mass system failure due to IT infrastructure compromise

Major Enterprise Cyber Exposures – Detailed Analysis and Risk Context

The complexity and interconnectivity of airline operational systems heighten the impact of cyber events, making traditional continuity planning insufficient without embedded cyber risk modelling. These exposures should be formally integrated into enterprise ISMS and BCP documentation, supported by robust detection, layered defenses, and scenario-based simulation testing.

1. Introduction This document presents an in-depth discussion of high-priority enterprise-level cyber exposures facing a modern airline operating critical aviation, operational, and commercial systems. These risks span multiple digital domains and reflect complex interdependencies among systems supporting flight safety, logistics, revenue operations, and business continuity.

2. Coordinated Ransomware Attacks on Operational Systems (EFB, OCC, DCS)
Exposure Overview: Ransomware campaigns targeting interconnected aviation platforms can paralyze core operations, especially when simultaneously affecting flight dispatch systems (OCC), Electronic Flight Bags (EFB), and Departure Control Systems (DCS).

Potential Impacts:

- Loss of real-time aircraft operational data
- Inability to dispatch aircraft or issue boarding passes

- Crew unable to access route briefs or MEL/CDL data via EFB

Examples:

- A synchronized ransomware attack encrypts OCC servers, DCS check-in terminals, and the crew EFB management platform, resulting in full network lockdown across three major hubs.
- Ransomware payload disables domain controller, forcing shift to paper dispatch and disrupting EFB configuration updates across fleet.

Risk Factors:

- Inadequate network segmentation between operations and support systems
- Unpatched vulnerabilities in legacy dispatch or DCS modules
- Weak endpoint protection on EFB ground sync stations

3. Data Corruption in ERP Affecting Maintenance, Logistics, and Payroll

Exposure Overview: Enterprise Resource Planning (ERP) platforms integrate vital administrative and operational functions. A cyber incident that corrupts these systems disrupts asset provisioning, financial integrity, and workforce availability.

Potential Impacts:

- Delays in aircraft parts ordering and delivery
- Inaccurate crew payroll, triggering industrial action or absenteeism
- Maintenance planners operating with corrupted inventory or shift data

Examples:

- Integrity attack on the ERP's logistics module alters scheduled delivery data, resulting in AOG scenarios at multiple stations due to unavailable rotables.
- Insider threat modifies payroll configurations, resulting in non-payment to over 2,000 staff and triggering HR system lockout.

Risk Factors:

- Lack of transactional audit logging in ERP workflows
- Overreliance on real-time API integrations without failover safeguards
- Poor separation of duties in finance-logistics access roles

4. Communication Outages Between Dispatch and ATC or Airports

Exposure Overview: Dependable communication between dispatch and Air Traffic Control (ATC) or airport stakeholders is critical for flight clearance, rerouting, and gate coordination. Cyber-physical or infrastructure threats can sever these channels.

Potential Impacts:

- Blocked flight departures or diversions due to lack of clearance
- Loss of visibility on gate assignments, runway usage, and emergency services
- Manual coordination via non-secure channels, increasing operational error risk

Examples:

- DDoS attack against airport operational networks affects integration with airline dispatchers; OCC unable to transmit revised flight plans for 18 departing flights.
- Fiber-cut sabotage event disrupts redundant ATC–airline data circuit; voice-only fallback used under time pressure introduces delays and risks.

Risk Factors:

- Single points of failure in airport network interconnection points
- Unprotected satellite or VoIP fallback systems
- Absence of secure, encrypted mobile coordination protocols as backup

5. Mass System Failure Due to IT Infrastructure Compromise

Exposure Overview: Catastrophic collapse of central IT infrastructure due to malware, firmware attacks, or insider sabotage can disrupt multiple service layers including ticketing, maintenance, and safety systems.

Potential Impacts:

- Outage of integrated airline platform including PSS, ERP, and maintenance systems
- Disruption of backups and DR due to simultaneous compromise of storage arrays
- Failure to meet regulatory reporting or compliance obligations within time limits

Examples:

- Advanced persistent threat (APT) implants firmware-level compromise in primary and backup data center arrays; results in system-wide failure and unavailability of clean restoration points.
- Privileged user credentials abused to disable backup routines and manipulate logging, obscuring incident timeline and extending downtime.

Risk Factors:

- Weak firmware monitoring and insufficient BIOS-level integrity checks
- Inadequate segregation of production and backup environments
- Delayed patching and unsupported hardware in critical data centers

4. Business Impact Analysis (BIA) All business units undergo enterprise-wide BIA to determine the impact of disruptions. Key high-impact domains:

- **Flight Dispatch & OCC:** Disruption delays aircraft release, crew rotation, and emergency management.
- **Passenger Service Systems (PSS):** Outages affect check-in, boarding, and customer care.
- **Digital Maintenance Systems:** Inaccessibility of AMOS/TRAX blocks defect rectification, jeopardising airworthiness.
- **Cargo & Ground Handling:** Data loss delays manifests, handling operations, and security oversight.

Business Impact Analysis (BIA) – Domain-Specific Exposure Assessment
1. Introduction This document provides a detailed assessment of critical business domains identified through enterprise-wide Business Impact Analysis (BIA). It outlines BIA-driven exposure analysis is essential for prioritizing cyber and continuity investments.

Effective mapping of impact scenarios to operational domains ensures resilience and safeguards airline safety, regulatory compliance, and customer trust.
the functional implications of system disruptions and highlights potential cyber and operational exposures that may impact continuity and resilience within the airline environment.

- Each critical domain must be supported by a tested recovery playbook including offline operational procedures.
- Risk registers should map each domain to associated threat vectors, control failures, and mitigation maturity.
- Prioritize redundancy and failover mechanisms for systems with high RTO/RPO sensitivity.

Flight Dispatch & Operations Control Centre (OCC)
Criticality: High – Real-time flight operations coordination, aircraft dispatch approval, and emergency management.
Potential Impacts:

- Delays in aircraft dispatch due to loss of real-time planning and weather/NOTAM data
- Crew misallocation and regulatory non-compliance on flight duty limits

- Degraded emergency response coordination with airports and regulatory bodies

Exposure Scenarios:

- **Malware in Dispatch Planning Tools:** Ransomware disables dispatch consoles and integrated flight-tracking dashboards.
- **Loss of Connectivity to Flight Planning Systems:** VPN or MPLS link outage isolates OCC from global dispatch network.
- **Authentication Failure:** Compromised AD credentials prevent dispatcher login to EFB data upload tools.

Passenger Service Systems (PSS)

Criticality: Very High – Interfaces with customer service, check-in, boarding, and real-time flight updates.

Potential Impacts:

- Check-in and boarding system failures lead to long queues, denied boarding, and delays
- Customer support platform unavailability affects flight rebooking and special services
- Loyalty system or ticketing data loss results in reputational damage and revenue disruption

Exposure Scenarios:

- **DDoS on Booking or Mobile Check-in Portals:** Traffic flood causes multi-hour denial of service at peak times.
- **Data Corruption in Departure Control System:** Boarding card mismatches cause passenger manifest errors.
- **Integration Failure with Airport Infrastructure:** Airport CUTE system unable to sync with airline DCS, delaying departures.

Digital Maintenance Systems (AMOS, TRAX, OASES)

Criticality: High – Supports compliance, airworthiness management, and daily aircraft serviceability.

Potential Impacts:

- Unavailability of AMOS/TRAX blocks issuance of work orders and task closures
- Loss of aircraft status data (defects, MEL, servicing) results in unsafe or illegal flight releases
- Compromised system integrity could mask serious technical issues

Exposure Scenarios:

- **Ransomware Attack on Maintenance Servers:** Locks maintenance records during heavy check.
- **Failed Backup Restoration:** Data loss prevents reconstruction of completed work pack history.
- **Unauthorized Data Manipulation:** Insider alters MEL/CAT data, falsifying airworthiness.

Cargo & Ground Handling Systems

Criticality: Medium to High – Tied to turnaround efficiency, manifest compliance, and safety-sensitive ramp operations.

Potential Impacts:

- Delay or loss of cargo manifests causes customs and loading disruptions
- Missing handling instructions lead to misloaded ULDs or unsafe ramp movements
- Disruption in real-time data feeds results in uncoordinated ground movements

Exposure Scenarios:

- **Loss of Access to Weight & Balance Systems:** Incorrect load sheet issuance jeopardizes flight safety.
- **Corrupted Digital Handling Checklists:** Ramp teams operate with outdated task sets, missing last-minute changes.
- **GSE Communication Loss:** Ground Support Equipment (GSE) telemetry cut-off causes inefficiencies and safety incidents.

Continuity Measures and Security Controls BCP implementation is structured around the following key areas:

Asset Protection and Physical Redundancy

- Biometric access control and 24/7 monitored server facilities
- Geographic data center redundancy
- Hardened endpoints and encrypted workstations **Exposure:** Physical breach or power loss at data center impacting core airline systems

Backup, Replication, and Data Recovery

- Daily automated backups of PSS, OCC systems, maintenance records
- Cloud-based and offsite hot standby environments

- Business unit–specific RTO and RPO targets **Exposure:** Restoration failure delays resumption of critical services (e.g., crew rostering)

Continuity Measures and Security Controls – Exposure Analysis and Implementation Review

Introduction Business Continuity Planning (BCP) in an airline enterprise environment is dependent on the integration of robust technical, physical, and procedural controls. This document provides a detailed discussion of the foundational continuity measures deployed and evaluates potential sources of cyber and operational exposure in each domain.

Continuity controls must operate under the assumption that both digital and physical systems may be targeted by sophisticated threat actors or exposed by environmental failure. The above measures, while robust, require continuous validation, monitoring, and testing to ensure readiness under actual operational stress.

Future updates should incorporate automated failover validation, cyber-physical simulation exercises, and integration with enterprise ISMS metrics.

Asset Protection and Physical Redundancy

Controls Implemented:

- **Biometric Access Control:** High-security authentication at data centers and IT control rooms to restrict physical access to authorized personnel.
- **24/7 Monitored Facilities:** Surveillance and on-site security to prevent intrusion, tampering, or insider misuse.

- **Geographic Data Centre Redundancy:** Dispersed infrastructure (at least two regions) to absorb failures from natural disasters, cyberattacks, or power loss.

- **Hardened Endpoints:** Devices configured with limited peripheral access, full disk encryption, and tamper-resistant hardware.

Exposure Scenarios:

- **Physical Breach of Server Rooms:** Compromised credentials or badge cloning allows unauthorized access to critical airline data repositories.

- **Localized Power Loss or Fire:** Single point of failure at primary facility without fully synchronized secondary site can disrupt operations.

- **Environmental Control Failure:** HVAC or fire suppression malfunction damages hardware despite physical security.
- **Endpoint Theft or Tampering:** Aircraft operations laptops or maintenance tablets stolen and exploited due to encryption misconfiguration.

Mitigation Recommendations:

- Conduct red-team physical penetration tests and improve sensor layering.
- Mandate dual-operator access policies for critical systems.
- Include generator backup, redundant cooling, and zoned fire controls in continuity design.

Backup, Replication, and Data Recovery

Controls Implemented:

- **Daily Automated Backups:** Scheduled backups of key systems such as PSS, OCC, maintenance tracking, finance, and crew rostering.
- **Cloud-Based and Offsite Replication:** Real-time or near-real-time replication to secure third party or secondary enterprise-controlled data centers.
- **Business Unit–Specific RTO and RPO Targets:** Defined recovery expectations by function (e.g., 4-hour RTO for dispatch; 24-hour RTO for HR/payroll).

Exposure Scenarios:

- **Restoration Failure Due to Corrupted Backups:** Backups contain undetected malware or configuration errors.
- **Unsynchronized Replication:** Delayed updates cause data inconsistency between production and standby systems.
- **Cloud Service Dependency Breach:** Third-party cloud provider suffers breach or outage, delaying data availability and breaching SLAs.
- **Improper Segregation of Backup Storage:** Simultaneous compromise of production and backup environments due to shared access controls.

Mitigation Recommendations:

- Use immutable (write-once) storage for critical backups with versioning.
- Regularly test restoration playbooks under time pressure and system load.
- Encrypt backups in transit and at rest, with key management decoupled from hosting provider.
- Perform external audits of cloud data handling and redundancy compliance.

IT & Communications Redundancy

- Dual-path internet and MPLS networks
- Satellite and mobile communication backup for OCC and ramp staff **Exposure:** Simultaneous loss of digital comms between OCC and AOC control towers

IT & Communications Redundancy – Exposure Analysis and Resilience Strategy

1. Introduction Reliable communication infrastructure is critical to airline operations, enabling coordination between Operations Control Centre (OCC), Airport Operations Centre (AOC), and air traffic control (ATC), ground handling, and flight crews.

Conclusion Redundancy is not immunity. True resilience in airline IT and communications infrastructure requires multilayered planning, operational simulation, and constant validation of fallback effectiveness.
By identifying and addressing gaps in digital communication continuity, the organisation safeguards flight safety, efficiency, and regulatory accountability in the face of complex disruptions.

Redundancy Controls Implemented

Dual-Path Internet and MPLS Networks:

- Primary and secondary circuits provisioned via separate ISPs or paths
- MPLS used for high-availability, secure private communications across OCC, AOC, and satellite bases
- Failover triggers set for automatic switching upon packet loss, latency spikes, or physical link disruption

Satellite and Mobile Communication Backup:

- Satellite phones, broadband terminals, and VPN-enabled mobile devices provisioned for OCC, ramp staff, and airport duty managers
- Alternate routing of voice and data traffic via LTE/5G during WAN failures
- Encrypted messaging and secure collaboration apps configured for fallback usage during primary system downtime

Exposure Scenarios and Impact

Simultaneous Loss of Digital Comms Between OCC and AOC:

- Both primary (fiber-based MPLS) and secondary (LTE/5G or satellite) links experience failure, degradation, or are targeted by cyberattack

Exposure Sources:

- **Cyber-Physical Attack:** Coordinated sabotage (e.g., fiber cuts or utility tampering) disables both primary and redundant terrestrial links
- **Satellite Signal Jamming:** Electromagnetic interference or GPS spoofing renders SATCOM unreliable during critical coordination
- **Mobile Network Saturation or Denial of Service:** Localized telecom failure (e.g., during airport emergency or mass disruption) causes cellular fallback to collapse under traffic load
- **Misconfigured Failover Policies:** Routing tables or firewalls fail to trigger switchover or introduce loopbacks during network transition

Operational Impacts:

- Inability to issue last-minute flight plan updates or coordinate diversions
- Delays in real-time transmission of MEL/CDL status to flight deck and ground crews
- Failure to manage airport turnaround or coordinate gate allocations during congestion or emergency
- Loss of situational awareness and delay in escalation to national aviation authorities

Mitigation Recommendations

- Conduct quarterly failover drills simulating full digital communication outage at airport and control center nodes

- Use separate physical paths, hardware vendors, and logical network segregation for redundant circuits
- Preload critical documents (e.g., diversion protocols, flight release forms) on local offline devices at OCC and AOC
- Deploy auto-healing SD-WAN configurations with pre-approved policy routing logic
- Ensure redundancy for SATCOM units, with backup terminal power and frequency shielding against jamming

Identity and Access Management (IAM)

- Federated IAM with role-based access across domains
- MFA, session monitoring, automatic access revocation **Exposure:** Privilege escalation attack during a crisis compromising core data flows

Secure Inter-System Communication

- TLS-encrypted APIs across ERP, PSS, CAMO/AMO platforms
- Enforced cybersecurity posture on vendor platforms (e.g., EFB, GSE telemetry) **Exposure:** Supply chain compromise introducing vulnerability into internal platforms

2. Identity and Access Management (IAM)
IAM and inter-system communication integrity are foundational to airline security architecture. They require not only strong baseline controls but also continuous reassessment to address evolving access misuse and integration vulnerabilities. A layered, role-aware, and vendor-conscious strategy is essential for maintaining operational and data security across the ecosystem.

Controls Implemented:

- **Federated IAM:** Centralized identity control using Single Sign-On (SSO) and directory federation across enterprise systems including ERP, OCC, PSS, AMOS, and eLearning platforms.

- **Role-Based Access Control (RBAC):** Access rights assigned by job function, with separation of duties across maintenance, finance, and operations.
- **Multi-Factor Authentication (MFA):** Mandatory for privileged accounts and remote access points.
- **Session Monitoring & Auto Revocation:** Automated detection of anomalous activity, with session timeout, forced logout on HR deactivation, and event-driven revocation (e.g., credential misuse).

Exposure Scenarios:

- **Privilege Escalation During Crisis:** Emergency account access workflows bypass standard approval logic.
  - *Example:* An attacker compromises a helpdesk account and uses 'break-glass' privilege elevation to modify OCC flight plan exports.
- **Orphaned Accounts Post-Contractor Off boarding:** Former third-party AMO engineer retains dormant credentials.
- **Credential Harvesting via Spear Phishing:** Targeted campaign exploits MFA fatigue or legacy login loopholes in under-monitored systems.
- **Access Role Creep:** Cross-functional personnel accumulate excessive rights over time, creating audit blind spots.

Mitigation Recommendations:

- Deploy just-in-time access provisioning with auto-expiry.
- Conduct quarterly access audits by department and asset sensitivity.
- Implement behavioral biometrics or step-up authentication for high-risk actions.
- Enforce tight conditional access policies (e.g., geo-fencing, time-based logic).

Secure Inter-System Communication

Controls Implemented:

- **TLS Encryption Across Interfaces:** Data exchanges between ERP, PSS, CAMO, AMO, and OCC platforms secured via HTTPS and encrypted APIs.
- **Vendor Cybersecurity Posture Assessment:** Third-party platforms integrated via audited gateways and contractual SLAs requiring encryption, access logging, and patch compliance.

- **Segregated API Gateways:** Critical data flows (e.g., maintenance deferrals, crew scheduling, loyalty accounts) protected by policy enforcement points with logging and rate limiting.

Exposure Scenarios:

- **Supply Chain Compromise:** Partner system integrated via API introduces malware or intercepts sensitive traffic.
  - *Example:* A trusted GSE telemetry vendor uploads a compromised firmware update, creating lateral movement into ground operations systems.
- **Outdated or Weak TLS Protocols:** API endpoints accept deprecated ciphers (e.g., TLS 1.0), allowing session hijacking.
- **Improper Token Management:** Static bearer tokens hardcoded in integration scripts lead to credential leakage.
- **Overprivileged APIs:** Lack of scope-based permissioning allows a non-critical service to extract PII from CRM datasets.

Mitigation Recommendations:

- Implement mutual TLS authentication and rotate certificates regularly.
- Use OAuth2 with dynamic access tokens and expiration logic.
- Vet all vendor systems via security questionnaires and sandbox validation prior to API enablement.
- Maintain a central API management platform with audit-ready logs.

Incident Detection and Integrated Response

Classification and Crisis Escalation Aligned with IS.I.OR.220 and internal ISMS protocol:

- **Severity 1 – Crisis Event:** Immediate BCP and emergency response activation
- **Severity 2 – Major Impact:** Partial degradation; recovery within 12–24 hours
- **Severity 3 – Localised:** Departmental interruption managed internally

Playbooks and Recovery Coordination

- Incident-specific runbooks (e.g., OCC system outage, ransomware, airport shutdown)

- Emergency Communication Centre activates redundant collaboration platforms (e.g., secure VoIP, SMS push)
- Business units follow standard fallback procedures for continuity

Testing and Validation

- Annual enterprise BCP simulation (ransomware, OCC failure, mass flight cancellation)
- Departmental tabletop exercises for localised scenarios

Incident Detection and Integrated Response – Exposure Analysis and Preparedness Framework

Introduction An effective Incident Detection and Response framework is central to ensuring the operational resilience of a modern airline.

Robust incident response and escalation systems are foundational to business continuity in the aviation sector. Continuous validation, clear severity mapping, and interoperable fallback communication channels ensure that crises are managed swiftly and decisively. Identifying exposures before a real event allows the organisation to transform vulnerabilities into operational resilience.

Classification and Crisis Escalation (Aligned with IS.I.OR.220)
Severity 1 – Crisis Event:

- **Definition: Enterprise-wide or safety-critical disruption requiring immediate activation of the BCP and Emergency Response Plan.**
- **Example: Simultaneous ransomware attack on OCC and PSS systems.**
- **Exposure:**
  - **Delayed or inaccurate classification due to overwhelmed monitoring systems.**
  - **Ineffective triggering of BCP if escalation matrix is outdated or key personnel are unavailable.**
  - **Miscommunication or command confusion due to non-aligned roles and contact lists.**

Severity 2 – Major Impact:

- **Definition: Significant operational degradation with functional recovery targeted within 12–24 hours.**
- **Example: Partial data corruption in ERP affecting maintenance scheduling.**
- **Exposure:**
  - **Inconsistent decision-making due to unclear recovery priorities between business units.**

- Resource contention for shared IT and recovery staff during multiple simultaneous incidents.
- Lack of visibility into upstream or downstream service impacts (e.g., effect of ERP delay on finance and rostering).

Severity 3 – Localised Incident:

- **Definition: Departmental or site-specific interruption manageable within local authority.**
- **Example: Ground handling system login failure at one airport.**
- **Exposure:**
  - **Incident under-reporting due to perceived low criticality.**
  - **Deferred response escalates into wider impact (e.g., security incident due to delayed aircraft loading).**
  - **Local teams bypass standard reporting channels, delaying enterprise awareness.**

Playbooks and Recovery Coordination

Controls Implemented:

- **Incident-specific runbooks including ransomware response, OCC outage recovery, airport IT system shutdowns, and data corruption events.**
- **Emergency Communication Centre (ECC) activation triggers parallel communication over redundant channels such as secure VoIP, SMS push, and encrypted collaboration apps.**
- **Standard fallback procedures (manual dispatch, paper check-in, etc.) are issued to business units for continuity.**

Exposure Scenarios:

- **Stale or Unvalidated Playbooks: Outdated procedures that assume non-existent systems or unavailable staff.**
- **Recovery Role Conflicts: Misalignment between ECC instructions and departmental SOPs leading to duplication or missed steps.**
- **Fallback Communication Platform Failure: Redundant comms system suffers overload or configuration error during initial switch.**
- **Lack of Interoperability Between Systems: Fallback systems are not synchronized, creating confusion in version control or flight release data.**

Testing and Validation –

Controls Implemented:

- **Annual organisation-wide simulations (e.g., ransomware impacting primary and secondary data centres).**

- **Tabletop exercises for business continuity scenarios such as mass flight cancellation, OCC cyber outage, and supply chain disruption.**
- **Post-exercise debriefings with gap analysis and action plan tracking.**

Exposure Scenarios:

- **Simulations Lack Realism: Exercises fail to simulate multi-domain complexity, limiting stress testing value.**
- **Inadequate Participation: Critical staff unavailable during testing; alternate personnel lack context or decision-making authority.**
- **Lessons Not Integrated: Findings from exercises not translated into policy, playbook updates, or procurement decisions.**
- **Non-Functional Testing Environment: Tabletop exercises not linked to system simulation tools, limiting realism and risk discovery.**

Recommendations

- **Implement automated incident severity scoring based on telemetry and business impact models.**
- **Maintain dynamic contact and escalation lists with automated personnel notification.**
- **Conduct surprise simulations and involve third-party observers to challenge assumptions.**
- **Review and update playbooks bi-annually with version control and stakeholder validation.**

7. Training, Awareness and Role-Specific Readiness

- Enterprise BCP and cyber resilience modules for all employees
- Specialist drills for OCC, IT Security, Maintenance Controllers, and Cabin Crew
- Live refresher and just-in-time training tools for emergency checklists **Exposure:** Role confusion during BCP activation resulting in miscommunication or delay

8. Audit, Performance Monitoring, and Continuous Improvement

- Regular ISMS audits incorporate BCP elements
- Metrics tracked: Recovery Point Objective (RPO), Recovery Time Objective (RTO), user communication delay, data loss thresholds
- Incident reports trigger formal root cause analysis, leading to policy and procedural upgrades

9. Regulatory Compliance and Assurance The BCP framework is harmonised with:

- Regulation (EU) 2023/203 and Delegated Regulation (EU) 2022/1645
- AMC/GM to IS.I.OR.200, 205, and 220
- IATA Operational Safety Audit (IOSA), ISO/IEC 27001, and ISO 22301 where applicable

Enterprise Level Risks for Assessment

Governance & Strategic Integration Risks

1. **Delayed Board-Level Threat Awareness** – Cyber incidents not escalated promptly, undermining strategic BCP decisions.
2. **Use of Shadow IT by Executives** – Unauthorized apps/devices bypass enterprise controls during crises.
3. **Fragmented Incident Playbooks** – Inconsistent or outdated departmental BCP guidance results in uneven recovery.
4. **Lack of Policy Harmonization Across Units** – Incoherent application of ISMS–BCP directives increases regulatory exposure.
5. **Third-Party Non-Conformance** – Suppliers fail to meet ISMS-related BCP controls (e.g., CRM or EFB vendors).

Operational Continuity Risks (OCC, Dispatch, Flight Ops)

6. **OCC Malware Compromise** – Ransomware or backdoors disrupt real-time dispatch operations.
7. **VPN/Comms Failure During Critical Operations** – Isolates dispatchers from ATC, triggering operational rerouting.
8. **Corrupted Crew Rostering System** – Leads to rest non-compliance and operational delays.
9. **Simultaneous OCC and ATC Link Loss** – Multi-point comms breakdown blocks coordination.

Maintenance & Airworthiness Systems

10. **Tampering with Deferred Defect Data** – Alters MEL/CDL logs, compromising airworthiness.
11. **Unrecoverable AMOS/Task Data Post-Outage** – Failed backup or replication halts scheduled maintenance.
12. **Loss of ARC Documentation** – Data deletion or integrity breach affects regulatory compliance.

Customer-Facing System Risks

13. **DDoS Against Booking/Check-in Portals** – Impacts brand reputation and revenue during peaks.
14. **CRM Exploitation** – Loyalty or payment data stolen due to third-party API weakness.
15. **Downstream Ticketing Platform Outage** – Third-party downtime cascades to DCS failure and boarding delays.

Safety-Critical Comms & Coordination

16. **Safety Reporting System Downtime** – Obstructs timely SMS hazard communication and incident escalation.
17. **ACARS Signal Manipulation or Loss** – Disrupts inflight telemetry and command updates.
18. **Access Denied to ERP/Crisis Coordination Tools** – Prevents coordinated response during multi-airport disruption.

Mass System/Infrastructure Risks

19. **Central IT Compromise (APT/Firmware)** – Impacts PSS, OCC, and Maintenance via domain controller or firmware attack.
20. **ERP Data Corruption** – Affects logistics, payroll, and crew management integrity.
21. **Simultaneous Backup & Production Breach** – Shared access undermines DR viability.

IAM & Inter-System Communication

22. **Privilege Escalation via Emergency Access Misuse** – “Break-glass” credentials exploited during chaos.
23. **Orphaned Third-Party Access** – Dormant AMO/CAMO credentials create persistent threats.
24. **Hardcoded API Tokens** – Static tokens in scripts allow lateral data access.
25. **Outdated TLS Across System Interfaces** – Enables session hijacking or MiTM attacks.

Redundancy & Physical Layer

26. **Simultaneous Failure of OCC Primary and Redundant Links** – Dual failure (e.g., MPLS and LTE) paralyzes control centers.
27. **Satellite Jamming or GPS Spoofing** – Blocks fallback comms, especially in remote or degraded ops.
28. **Power Loss Without Proper Failover** – Single-point outage disables primary systems without effective failover.
29. **Server Room Physical Breach** – Insider threat or cloned credentials used to access protected systems.
30. **Stolen or Compromised Mobile Devices (EFB, Ramp Tablets)** – Devices exploited due to insufficient encryption or revocation.

Incident Response, Training & Continuous Improvement

31. **Delayed Incident Escalation** – Incorrect severity classification delays BCP activation.
32. **Unvalidated or Outdated Playbooks** – Procedures reference obsolete systems or roles.
33. **Inadequate Cross-Role Training** – Leads to execution failure during real events (e.g., crew briefings or system recovery).
34. **Non-Translated Lessons from Simulation Exercises** – Findings not reflected in ISMS–BCP updates or procurement.
35. **Audit Non-Conformance (ISMS–BCP Alignment)** – Internal audits reveal repeated policy or control failures.

These risks should be mapped to:

- **Risk owner**
- **Threat vector/source**
- **CIA triad impact analysis**
- **BCP dependency (e.g., OCC, AMOS, PSS)**
- **Control assessment and residual exposure**
- **Treatment strategy** (mitigate, accept, transfer, avoid)