AIRPORTS COUNCIL INTERNATIONAL

Airport Cyber Security Governance

ACI EUROPE GUIDANCE DOCUMENT

ACI EUROPE
Cybersecurity Committee

TLP: CLEAR

Table of contents

1. Document Control

Document Details

Document Title	Airport Cyber Security Governance
Document Number	202502
Classification	TLP CLEAR
Version Number	1.0
Status	Active

Author & Owner Details

Author	ACI EUROPE Cyber Security Committee
Owner	ACI EUROPE
Approved For Release By	ACI EUROPE Aviation and Cyber Security Director

Next Review Date

Next Review Date	N/A

Version History

Version	Date	Comments	Reviewed by
0.1	23/07/2025	First draft	Cyber Governance WG
0.2	01/10/2025	Incorporation of Comments + ACI EUROPE Edits	Cyber Governance WG
0.3	07/11/2025	Update following 4th meeting of the Cyber Security Committee	ACI EUROPE
0.4	23/12/2025	Final draft	Cyber Governance WG
0.5	12/01/2025	Version ready for publication edits	Cyber Governance WG
1.0	27/01/2026	Release Version	ACI EUROPE

2. Executive Summary

This document aims to establish a scalable, adaptable cybersecurity governance framework tailored to airports of varying sizes, from small regional airports to large international hubs and multi-airport groups. It provides practical guidance, clearly defined roles, and structured reporting practices to enable effective oversight, risk mitigation, and compliance.

The framework supports airports in:

- Enhancing resilience against cyber threats across IT, OT, and physical security domains,
- Aligning with principles described in the NIS2 directive,
- Strengthening executive and board-level engagement through tiered reporting models,
- Enhancing strategic and operational decision-making related to cybersecurity
- Aligning cybersecurity strategy with aviation-specific regulatory requirements and global best practices,
- Fostering a unified, risk-driven, and security-conscious culture across airport environments.
- Promoting coordination between cybersecurity and physical security domains.
- Facilitate continuous improvement and maturity of airports' cybersecurity posture.

Commented [SC1]: already included in the title above

This guidance document provides best practices and recommendations that are not intended to contravene national regulations or override airport-specific operational, organisational, or contextual realities, and should not be interpreted as prescriptive or binding.

3. Acknowledgement

ACI EUROPE would like to extend its sincere appreciation to the members of the Cyber Security Committee for their valuable input and contribution to this document. A special thanks goes to Panagiotis Merkouris, Head of Information Security at Athens International Airport S.A., for his active involvement, thoughtful guidance, and steady commitment throughout the development of this guidance. His dedication and expertise greatly helped shape a document that supports airports in strengthening their cybersecurity practices and resilience.

The ACI EUROPE Cyber Security Committee serves as a strategic advisory body to the ACI EUROPE Board, both on its own initiative and at the Board's request. Acting as a think-tank within its area of expertise, the Committee identifies key strategies, stakeholders, priorities, regulatory initiatives, and policies related to cybersecurity in the airport industry. It helps members comply with relevant regulatory requirements and safeguard their ability to operate by promoting higher cybersecurity maturity across the air transport sector. Additionally, the Committee monitors and analyses emerging cybersecurity challenges and trends affecting airports. A key part of its mission is to foster a "system of trust" among ACI EUROPE members

by encouraging the open exchange of experiences, best practices, and information on cybersecurity incidents.

4. Reference Documents

To ensure alignment with industry best practices and regulatory requirements, the following documents have been considered:

- **ICAO Cybersecurity Policy Guidance:** Guidelines for the protection and resilience of critical infrastructure against cyber threats within international civil aviation.
- **Doc 10213 — Unrestricted Global Cyber Risk Considerations:** Assists Member States and stakeholders in integrating cyber risk management into their aviation risk management processes.
- **Cybersecurity Implementation Handbook:** Offers practical guidance for airports to enhance their cybersecurity posture.
- **Aviation Cyber Security Guidance Material** (Part 1: Organization Culture and Posture; Part 2: Aircraft operations and risk management).
- **Directive (EU) 2022/2555 "NIS2";** includes obligations for Member States to develop mandatory risk management principles for identified entities, supply chain security, incident reporting, and personal liability for senior management.
- **European Union Aviation Safety Agency (EASA) Regulations (e.g., EU 2023/203 & EU 2024/2690):** Focusing on information and cybersecurity in aviation.
- **NIST Cybersecurity Framework (CSF):** A widely adopted framework for improving critical infrastructure cybersecurity.
- **ISO/IEC 27001:2022 Standard – Information Security Management Systems:** Provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system.
- **ENISA Guidelines on Securing Airport Infrastructure:** Provides guidance to airport decision-makers and security personnel on enhancing cybersecurity in airport environments.
- **ISO/IEC 27014**: A Framework for governing information security, ensuring alignment with business objectives, accountability at the leadership level, and effective oversight of the ISMS.
- **ENISA Cybersecurity Roles and Skills for Essential and Important Entities:** Supports organisations designated as essential or important under the NIS2 Directive in identifying, recruiting, and developing cybersecurity staff.
- **ENISA European Cybersecurity Skills Framework Role Profiles:** A common European reference framework for defining, classifying, and understanding cybersecurity professional roles and competencies.

5. Principles of Cybersecurity Governance in Airports

Effective cybersecurity governance in airports is guided by principles such as:

- **Executive Oversight and Independent Reporting:** Cybersecurity should be recognised as a strategic function with appropriate independence from IT and should have direct visibility to executive management or the Board to enable objective oversight, effective risk-based prioritisation, and alignment with organisational objectives.
- **Leadership and Accountability**: Cybersecurity must be a strategic priority championed at the highest organisational levels, with clear expectations and accountability for outcomes.
- **Risk-Driven Approach**: Governance should be based on a comprehensive understanding of cyber risks, their potential impact, and the organisation's risk tolerance, prioritising investments based on this assessment.
- **Integrated and Holistic Security**: Cybersecurity should be embedded across all layers of airport operations, including physical security, information security (IT), operational technology (OT), human factors, and third-party relationships, for enhanced resilience.
- **Continuous Improvement**: Governance must support ongoing evaluation and refinement of cybersecurity controls, policies, and practices, given the evolving nature of cyber threats.
- **Compliance by Design**: Cybersecurity frameworks and controls should inherently meet applicable national and international regulations, standards, and industry best practices.
- **Security-Conscious Culture**: A strong security culture is essential and should engage all employees through awareness programs, training, and incentives.
- **Supply Chain and Third-Party Risk Management:** Airports must proactively assess and manage cybersecurity risks from vendors, contractors, and other third parties.

6. Governance and Reporting

A. Governance

ACI EUROPE endorses the *"ENISA – Cybersecurity Roles and Skills for Essential and Important Entities"* framework. From an airport security perspective, it is important to ensure that the Safety Manager role is also represented in the roles and skills table, reflecting the close interconnection between safety and cybersecurity responsibilities in airport operations.

Activity	Responsible	Accountable	Supporting	Consulted	Informed
A central point of contact for internal and external parties on information and cyber security.	CISO	Executive management	Information Security Manager		Board of directors, Safety Manager
Builds board and executive level awareness of cyber security risks and threats to the organisation.	CISO	Executive management	Information Security Manager	Other business units and subject matter experts, Safety Manager	Board of directors
Establishes and embeds the required cyber security culture.	Executive management	Board of directors	CISO	Cyber security steering committee, Safety Manager	All staff
Provides strategic cyber security direction and advice to the board.	Executive management	Board of directors	CISO	Information Security Manager, Safety Manager	
Interfaces with the board/executive management on strategic security initiatives and provides feedback.	CISO	Executive management	Information Security Manager	Other business units and subject matter experts, Safety Manager	
Defines and implements information and cyber security strategies.	CISO	Executive management	Information Security Manager	Cyber security steering committee, Safety Manager	Board of directors
Budgeting and acquisition of security funding.	CISO	Executive management		Cyber security steering committee, Safety Manager	Board of directors
Provides security leadership in cross-functional business and security teams.	CISO	Executive management	Information Security Manager	Safety Manager	

Activity	Responsible	Accountable	Supporting	Consulted	Informed
Develops and maintains cyber security architecture.	Information Security Manager	CISO		Other business units and subject matter experts, Safety Manager	Executive management
Defines relevant cyber security regulatory and compliance requirements.	Legal	Board of directors	CISO	Legal counsel, Safety Manager	Information Security Manager
Ensures physical security of critical IT/OT infrastructure (e.g., server rooms, control centers, communication cabinets).	Physical Security Manager	Executive Management	Facilities Management	CISO, ISM, Safety Manager	Board of Directors
Implements and maintains physical access controls (e.g., badge systems, biometrics) integrated with cybersecurity protocols.	Physical Security Manager	Executive Management	IT Operations	CISO, OT Lead, Safety Manager	All staff
Monitors and responds to physical breaches that could impact cybersecurity (e.g., unauthorized access to network closets).	Physical Security Operations	Physical Security Manager	CISO	Incident Response Team, Safety Manager	Executive Management
Conducts joint physical-cybersecurity risk assessments for interconnected systems.	CISO & Physical Security Manager	Executive Management	Risk Management Team	OT Engineers, ISM, Safety Manager	Board of Directors
Coordinates emergency response involving both cyber and physical security incidents.	Emergency Response Lead	Executive Management	Physical Security & CISO	Incident Response Team, Facilities, Safety Manager	All stakeholders

B. Report to Key Stakeholders

Effective reporting is crucial for maintaining informed decision-making and ensuring accountability in cybersecurity governance. Reports should be tailored to the audience, focusing on relevant information and avoiding excessive technical jargon.

i. Board of Directors

The Board requires a strategic, high-level overview focusing on business implications, reputation, and long-term sustainability. Topics include key risks, threat landscape, incidents, audit results, and strategic initiatives.

Topics to Report:

- **Key Cybersecurity Risks:** Identification of the most significant cyber risks facing the airport, their potential impact (financial, operational, reputational), and mitigation strategies. This should align with the airport's overall enterprise risk management framework.
- **Threats Landscape & Compliance Risk:** Updates on current and emerging threats, significant changes in cybersecurity laws, regulations, and industry standards, and the airport's compliance status.
- **Security Incidents & Threat Intelligence:** High-level quantified **o**verview of recent cybersecurity incidents affecting the airport, its partners, or the aviation industry.
- **Audit & Penetration Testing Results:** Summary of key findings from internal and external audits, vulnerability assessments, and penetration testing, with emphasis on systemic risks, progress in remediation, and areas needing executive attention.
- **Strategic Initiatives & Project Progress:** Updates on major cybersecurity projects and initiatives, including progress dashboards reflecting budget execution, achieved benefits, encountered challenges, and future milestones.
- **Cyber Risk Landscape & Rating:** A high-level overview of the most significant cybersecurity risks facing the airport, current and emerging threats, and the organisation's cyber risk rating (e.g., from external assessors), benchmarked against peers and competitors.

How to Report:

Category	Details
Frequency	Quarterly or at least semi-annually
Format	Executive summary, dashboards with key performance indicators (KPIs) and key risk indicators (KRIs), clear graphical representations of trends. Avoid technical jargon.
Focus	Strategic implications, financial impact, reputational risk, regulatory compliance, and alignment with business objectives.
Actionable Insights	Provide clear recommendations for board decisions or strategic direction.

ii. Audit Committee

The Audit Committee usually focuses on the effectiveness of internal controls, risk management processes, and financial implications.

Topics to Report:

- **Effectiveness of Cybersecurity Controls:**
  - Assessment of the design and operating effectiveness of key cybersecurity controls. This can include results from internal audits, external assessments, and penetration tests.
  - Include reporting on how the board and audit committee are maintaining executive oversight and board engagement over these controls.
  - Highlight any initiatives related to continuous education and expertise development for directors concerning cybersecurity controls and their effectiveness.
- **Risk Management Process:**
  - Review of the airport's cybersecurity risk assessment methodology, risk register, and ongoing risk management activities.
  - Emphasise the integrated risk management and disclosure approach, ensuring cybersecurity is treated as a strategic risk, not solely an IT function.
  - Report on the alignment of the airport's cybersecurity governance with evolving disclosure requirements.
  - Discuss how the proactive, risk-driven approach covers all layers of airport operations, including physical security and operational technology (OT).
- **Compliance with Audit Findings:** Status of remediation efforts for cybersecurity-related audit findings (internal and external).
- **Third-Party Cybersecurity Risk Management:**
  - Detailed review of the processes for assessing and managing cybersecurity risks posed by vendors and suppliers.
  - Consider reporting on the continuing education and expertise development efforts that equip the committee to understand and oversee the complexities of supply chain cybersecurity and how they fit within the broader integrated risk management and disclosure framework.
- **Incident Response Effectiveness:**
  - Post-incident review of the effectiveness of incident response processes, including lessons learned and improvements.
  - Report on how executive oversight and board engagement is maintained throughout the incident response lifecycle, ensuring clear accountability and effective communication channels for post-incident reviews and the implementation of lessons learned.

- **Fraud and Financial Impact:**
  - Any cybersecurity incidents that have or could have a significant financial impact, including potential fraud or extortion attempts.
  - Report on how the board's executive oversight and integrated risk management processes are designed to identify, assess, and mitigate cybersecurity incidents with potential financial implications, and how these are communicated to the audit committee as a top priority.

How to Report:

Category	Details
Frequency	Quarterly
Format	Detailed reports with specific control deficiencies, audit findings, risk ratings, and remediation plans.
Focus	Internal controls, compliance, financial impact, risk mitigation effectiveness, and assurance.
Evidence-Based	Support assertions with data, audit reports, and test results.

iii. Executive Management

Executive Management requires both strategic and operational insights to make informed decisions on resource allocation and operational priorities.

Topics to Report:

- **Operational Cybersecurity Metrics (KPIs):** Key performance indicators such as number of incidents, time to detect, time to respond, vulnerability remediation rates, security awareness training completion rates, phishing click-through rates, with relevant links to business continuity and overall organisational performance. **Overall Cybersecurity Posture & Maturity:** A summary of the airport's current cybersecurity maturity level against industry benchmarks or established frameworks (e.g., NIST NIS2, ISO 27001) and progress towards desired maturity.
- **Current Threat Landscape & Vulnerabilities:** Detailed intelligence on current and emerging threats, significant vulnerabilities identified in airport systems (IT, OT, IoT), and mitigation status.
- **Incident Management Overview:** Summary of all cybersecurity incidents, including status, impact, and resolution. Trend analysis of incident types and severity.
- **Security Project Status:** Updates on the progress of ongoing cybersecurity projects and initiatives, including timelines, budgets, and challenges.
- **Security Architecture & Technology:** Overview of deployed security technologies, their effectiveness, and plans for future technology investments.
- **Security Awareness & Training Program Effectiveness:** Metrics on employee participation, effectiveness of training, and areas for improvement.

- **Budget vs. Actual Spend:** Detailed review of cybersecurity expenditure against budget.
- **Legal & Regulatory Compliance**: Status of compliance with applicable cybersecurity regulations (e.g., NIS2, Part-IS, national aviation security requirements), audit findings, and remediation efforts

How to Report:

Category	Details
Frequency	Monthly or Bi-weekly for critical incidents; Quarterly for strategic reviews.
Format	Dashboards, detailed reports, presentations with drill-down capabilities.
Focus	Operational performance, risk mitigation, resource utilization, and progress towards objectives.
Action-Oriented	Identify areas requiring executive decision or intervention.

7. Interaction between Information Security, Aviation Security, and Safety Governance

The integration of Information Technology (IT), Operational Technology (OT), and physical security systems in airport environments has created a highly interconnected and complex security ecosystem. A breach in one domain, cyber or physical, can significantly impact the other. A holistic, integrated security approach that unifies the cyber and physical domains is essential to safeguard airport operations, infrastructure, and passengers.

A. Convergence of Systems and Shared Risks

- **Interconnected Infrastructure**: Modern airports depend heavily on a broad range of digital and physical systems. IT systems support passenger information, ticketing, and airline operations. OT systems underpin critical airport functions, including baggage handling, air traffic control, power distribution, and building automation. Physical security systems, including CCTV, access control, and intrusion detection, are now IP-enabled and rely on shared network infrastructures. This convergence increases the potential for cross-domain vulnerabilities.
- **Common Attack Vectors**: Threat actors can exploit the interplay between cyber and physical domains:
    - *Cyber-to-Physical Attacks*: A cyberattack on a Building Management System (BMS) could disrupt HVAC, fire suppression, or power systems, endangering safety and continuity. Attacks on baggage handling or air traffic control systems could paralyse airport operations or lead to catastrophic incidents.
    - *Physical-to-Cyber Breaches*: Unauthorised access to network closets or data centres can allow direct tampering with IT or OT systems, bypassing digital

defences. Physically compromising surveillance cameras or terminals may enable attackers to disable monitoring or plant malware.

- **Data Sharing and Security**: Physical security systems generate valuable data (e.g., video recordings, access logs) that must be protected against cyber threats. If compromised, this data could reveal sensitive operational details or hinder incident response. Conversely, cybersecurity intelligence can support physical security, such as by triggering increased patrols in response to detected anomalies.
- **Joint Risk Assessments**: Comprehensive security risk assessments must evaluate both cyber and physical vulnerabilities, especially when one domain may serve as a conduit for compromising another. For example, evaluating the cybersecurity of badge readers or the physical risks to a server room is essential for identifying interdependent threats.

B. Key Areas of Interaction

- **Access Control**:
  - *Physical Access to Cyber Assets*: Securing physical access to data centres, server rooms, and control rooms is a critical component of cybersecurity. This includes multi-factor authentication, hardened enclosures, surveillance, and real-time access monitoring.
  - *Cybersecurity of Access Control Systems*: Physical access control systems, such as smart card readers or biometric scanners, are often network-connected and susceptible to cyber threats. These systems must be protected against unauthorised access, tampering, and denial-of-service attacks.
- **Surveillance Systems (CCTV)**:
  - *Cybersecurity of Surveillance Equipment*: IP cameras and Network Video Recorders (NVRs) are increasingly targeted by attackers. Protecting them requires secure configurations, timely software updates, complex passwords, and network segmentation.
  - *Physical Protection of Surveillance Assets*: Cameras and surveillance infrastructure must be shielded from physical tampering or sabotage to ensure operational continuity.
- **Operational Technology (OT) Security**:
  - OT systems underpin critical airport operations from lighting and HVAC to baggage and air traffic control. Many OT systems are legacy-based, operate in real time, and use proprietary protocols, which makes securing them challenging.
  - Effective collaboration between IT security professionals and OT engineers is essential to implement safeguards such as segmentation, patching, intrusion detection, and real-time monitoring without disrupting operations.
- **Insider Threat Mitigation**:
  - Insider threats, whether intentional or accidental, pose significant risks. Mitigating these threats requires coordinated monitoring of both cyber and physical behaviours. Integrating identity and access management,

behavioural analytics, and anomaly detection across domains can help identify warning signs early.

- **Emergency Response Coordination**:
  - During major incidents, seamless coordination between cyber and physical response teams is vital. Integrated communication protocols, joint training exercises, and unified command structures enhance the ability to contain threats, minimise impact, and ensure rapid recovery.

8. Three-Tiered Cybersecurity Governance & Reporting Framework

This tiered model tailors cybersecurity governance and reporting practices to the airport organisation's size and complexity. The tiered model is based on the ACI EUROPE airport grouping system:

- Majors include airports with over 40 million passengers.
- Mega airports consist of those serving 25 to 40 million passengers.
- Large airports are comprised of airports with 10 to 25 million passengers.
- Medium airports serve 1 to 10 million passengers.
- Small airports cover airports with fewer than 1 million passengers.

Tier 1: Small Airports

Definition: Airports handling less than 1 million passengers per year and/or low cargo traffic, typically serving regional or remote areas. These airports usually operate with limited IT/OT infrastructure, fewer specialised cybersecurity resources, and lower exposure to targeted cyber threats.

Governance Emphasis:

- Assign cybersecurity responsibilities to a designated senior leader (e.g., Operations Director or CIO).
- Designate a simplified CISO role combining the responsibilities of the NIST Cybersecurity Risk Manager and Cyber Legal, Policy and Compliance Officer.
- Apply a simplified version of standard frameworks (e.g., NIST CSF, Mapping NIS2 obligations to ECSF-ENISA, ISO/IEC 27001).
- Prioritise awareness, essential technical controls, and third-party risk oversight.

Reporting Requirements:

- Semi-Annual Report to Executive Management: Cyber risks, incidents, and compliance status.
- Annual Report to the Board: Strategic summary including key risks, major incidents, and resource needs.
- Ad-hoc Incident Reports within 48 hours to the executive sponsor.
- Staffing: May rely on outsourced or part-time CISO services.

Tier 2: Medium and Large Airports

Definition: Airports with 1 to 25 million passengers per year. These airports have more complex operational environments, including multiple IT/OT systems and third-party integrations, making them moderately exposed to cyber risks.

Governance Emphasis:

- Full cybersecurity governance structure with defined roles for Board, Executive Management, CISO, and supporting departments.
- Implement dedicated roles for CISO, Cyber Incident Responder, Cybersecurity Implementer, and Penetration Tester
- Adopt mature cybersecurity frameworks (NIST, ISO/IEC 27001, EASA/EU regulations, Mapping NIS2 obligations to ECSF-ENISA).
- Integrate physical and cyber domains under a unified risk strategy.

Reporting Requirements:

- Quarterly Reports to the Board: Cyber posture, risks, incidents, and strategic project updates.
- Monthly Reports to Executive Management: KPIs, threat landscape, project milestones, and budget tracking.
- Annual Review by the Audit Committee: Audit findings, third-party risk, and control effectiveness.
- Staffing: Dedicated internal CISO with an independent reporting line to Executive Management.

Tier 3: Mega, Major and Network Operators

Definition: Airports with above 25 million passengers per year or airport networks operated under a single organisational structure handling a large volume of passengers per year. These entities often manage multiple airports across regions or countries, with advanced infrastructure, interdependent systems, and higher cyber threat exposure. They typically require enterprise-wide cybersecurity governance and risk management strategies.

Governance Emphasis:

- Establish a centralised cybersecurity function (e.g., Group CISO).
- Create a Group Cybersecurity Governance Board to oversee strategy and standardisation.
- Implement mature cybersecurity frameworks (NIST, ISO/IEC 27001, EASA/EU regulations, Mapping NIS2 obligations to ECSF-ENISA)
- Standardise reporting and cybersecurity practices across all airports.

Reporting Requirements:

- Quarterly Group-Level Report: Consolidated risk, incidents, benchmarking across airports.
- Standardised Local Reports: Consistent format for reporting from individual airports.
- Cross-Site Dashboards: Group-wide KPIs, threat intelligence sharing, risk heatmaps.
- Staffing: Group-level cybersecurity team with designated leads at each airport.