information

MDPI

Article

Aviation Cybersecurity Governance: Towards an Operational Framework and Solutions Agenda for the Airport Domain

Bilgin Metin [1], Hasan Burak Dümer [1] and Martin Wynn [2,*]

[1] Department of Management Information Systems, Bogazici University, Bebek, Istanbul 34342, Turkey; bilgin.metin@bogazici.edu.tr (B.M.); burak.dumer.2021@alumni.bogazici.edu.tr (H.B.D.)
[2] School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL502RH, UK
* Correspondence: mwynn@glos.ac.uk

Abstract

In an era where digital transformation shapes the backbone of global aviation infrastructure, the cybersecurity of air transport systems is of paramount importance. This article assesses the complex cybersecurity landscape within the civil aviation ecosystem, with a specific focus on the airport domain. The study first maps the vulnerabilities undermining airport operations by synthesizing secondary sources and industry reports (2015–2025) into a provisional conceptual framework (PCF). Then, this framework was operationalized and validated through primary research involving in-depth interviews with ten senior industry practitioners. These practitioner insights inform a comprehensive solutions agenda and an operational governance framework based on Governance, Risk, and Compliance (GRC) principles. By adopting a multifaceted Technology–People–Organization approach, the presented cybersecurity governance framework can ensure safe and sustainable airport operations through a continuous identify–implement–monitor improvement cycle. The findings provide both theoretical depth and practical relevance for airport operators and researchers aiming to fortify the aviation ecosystem against evolving digital threats.

Keywords: aviation; cybersecurity; governance risk compliance; GRC; airline operators; airport domain; vulnerabilities; GRC framework; human factors; cybersecurity governance

1. Introduction

Cybersecurity in aviation is critically important because it safeguards the integrity, availability, and confidentiality of the highly interconnected and digitalized systems that underpin the aviation industry. This includes everything from air traffic control systems, aircraft navigation and communication, passenger information, airport management systems, and ticketing services that together can be conceptualized as the aviation ecosystem. Given the potential for catastrophic outcomes, protecting these systems from cyber threats is vital for ensuring passenger safety, securing sensitive data, and maintaining trust in global air travel networks. As the aviation sector continues to embrace digital transformation, the need for cybersecurity measures grows exponentially to counteract the increasing sophistication of cyber threats and to prevent disruptions that could lead to significant financial losses and harm to public safety and national security [1].

Many aviation operators struggle with implementing consistent cybersecurity measures across their global supply chains. Almost a decade ago, Cooper [2] highlighted the problems emerging due to the growing international connectivity of the technologies and systems used throughout the industry. This increased connectivity, whilst engendering

Academic Editor: Jairo A. Gutierrez

Received: 9 November 2025
Revised: 6 January 2026
Accepted: 2 February 2026
Published: 10 February 2026

operational efficiencies, also expanded the attack surface for cyber threats. For example, the agreements for sharing Passenger Name Records (PNR) between countries have led to cyberattacks on this data, substantial financial losses for airlines, and severe compromises of passenger data. Such vulnerabilities necessitate stringent cybersecurity measures and protocols to safeguard sensitive passenger information and operational data [3].

Żmigrodzka [4] highlighted the critical vulnerability of the civil aviation sector to cyber threats, advocating robust international collaboration and the establishment of harmonized cybersecurity frameworks to ensure the sector's resilience against these evolving threats. Similarly, Ukwandu et al. [5] delineate the aviation industry's heightened vulnerability to state-sponsored actors and sophisticated cyberattacks, underscoring the necessity for robust, multi-layered security strategies capable of countering these advanced threats. The rapid evolution of cyber threats requires the aviation industry to constantly refine and expand its cybersecurity strategies. Janson [6] emphasizes the importance of a multi-layered approach to cyberspace monitoring in the U.S. aviation industry, utilizing advanced technologies and fostering collaboration among industry stakeholders to address emerging cyber threats effectively. This approach not only aims to pre-empt cyber threats but also ensures rapid response and recovery from incidents to minimize operational disruptions. However, as Hilderman [7] recently noted, although "many airlines and airports are beginning to adjust, in many cases security is still behind what it should be" (para. 4).

There is thus a pressing need for international consensus and coordinated action to combat cyber-terrorism and cyber-crime in the aviation ecosystem. Crafting an international cybersecurity strategy for civil aviation is crucial, encompassing human, technological, and process domains and requiring appropriate application methods [8]. The proactive endeavours of organizations like the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA) underscore the global aviation community's dedication to fortifying cybersecurity defences via collective action and the adoption of shared standards.

In Europe, the European Centre for Cybersecurity in Aviation (ECCSA) [9] plays a critical role in safeguarding aviation against cyber threats, promoting best practices to build a resilient and secure aviation ecosystem. The Société Internationale de Télécommunications Aéronautiques (SITA) [10], founded in 1949, is one of the most reliable institutions within the industry, offering information security services that protect airport and airline networks, IT systems, data, and users against cybersecurity threats. As the industry has become more reliant on technology, ICAO has expanded the scope of its activities to protect the entire air transport sector. Several resolutions of the ICAO Assembly [11] emphasize the importance of addressing cybersecurity within civil aviation. The ICAO Aviation Cybersecurity Strategy [12] aims to make the global aviation sector more resistant to cyberattacks, ensuring safety and security while allowing for continued innovation and growth. Furthermore, ICAO's Cybersecurity Policy Guidance [13] focuses on protecting critical aviation infrastructure from cyber threats. It stresses the need for cooperation within the aviation industry and with outside organizations like the military and national security agencies.

The UK Civil Aviation Authority (UKCAA) [14] has developed guidelines and regulatory requirements to address cybersecurity risks in the UK aviation sector. They actively manage and revise these regulations to ensure the protection of critical information systems from cyber threats, thereby playing a crucial role in leading cybersecurity efforts within the aviation industry. The UKCAA's Cyber Security Oversight Process for Aviation [15], known as CAP1753, serves as the foundational framework for all cybersecurity oversight activities. This process outlines comprehensive guidelines and best practices for enhancing cybersecurity resilience within the aviation sector. These guidelines are structured around four key objectives: ensuring effective governance and accountability, securing critical

information and communication technology systems, maintaining operational resilience, and fostering a proactive cybersecurity culture. By adhering to these objectives, the UKCAA aims to mitigate cyber threats and enhance the overall security posture of the aviation industry, safeguarding it against evolving cyber risks.

Within the aviation ecosystem, there are three main domains of activity that are conceptually and physically different, although there is some overlap: airports (and airline operators), aircraft, and air traffic control. In this research, the main focus is the airport domain, although some of the findings also touch upon the other two domains. What is currently missing is a comprehensive and practical airport domain cybersecurity framework, with an appropriate structure for risk governance and compliance, that recognizes the multiple dimensions of cybersecurity vulnerabilities and puts forward appropriate management solutions and measures. This article attempts to fill this gap in the academic and practitioner literature and more specifically addresses the following research objectives (ROs):

RO1: To develop a provisional conceptual framework (PCF) for subsequent analysis of cybersecurity vulnerabilities in the airport domain.

RO2: To classify the key cybersecurity vulnerabilities in the airport domain based on the PCF.

RO3: To establish and validate a framework for the governance of cybersecurity in the airport domain with a solutions agenda and action list.

This article comprises four sections. Following this introduction, the research method for the study is outlined, including profiles of the interviewees who provided the primary data for the study. Then, in Section 3, the three research objectives are directly addressed, drawing upon an analysis of pertinent literature and practitioner interviews. Finally, Section 4 provides a conclusion to the study and looks to future research initiatives that can contribute to continued vigilance and development of cybersecurity in the aviation ecosystem.

2. Research Method

The research process comprised three main phases (Figure 1). These are discussed in turn below.

Phase 1 involved a narrative (or integrative) literature review to assess and integrate existing research and industry knowledge on aviation cybersecurity governance. The objective of the review was to identify recurring challenges and conceptual dimensions that could inform the development of an operational framework for cybersecurity governance in the airport domain. Literature searches were conducted across major academic databases, including Scopus, Web of Science, ScienceDirect, and IEEE Xplore, as well as sector-specific and policy repositories such as ICAO, ENISA, and publications from Civil Aviation Authorities. The searches incorporated key terms including “aviation cybersecurity”, “airport cybersecurity”, “air transport information security”, “vulnerabilities”, “governance”, and “risk management”. Publications and reports from the years 2015 to 2025 were included to ensure coverage of both historical and contemporary aspects of the topic. The narrative review adhered to the methodological guidance proposed by Snyder [16], allowing for flexibility in integrating findings from both academic and practitioner sources to develop a conceptual understanding of the field. Snyder [16] notes the aim of such reviews is “to assess, critique, and synthesize the literature on a research topic in a way that enables new theoretical frameworks and perspectives to emerge” (p. 335). This provided the basis for the development of a provisional conceptual framework (PCF) that was then used in the subsequent research phases. The narrative review was seen as “a means of gaining an

initial impression" [17] (p. 97), which was used "to draw the big picture" [18] (p. 1) and provide a foundational understanding of the key concepts.

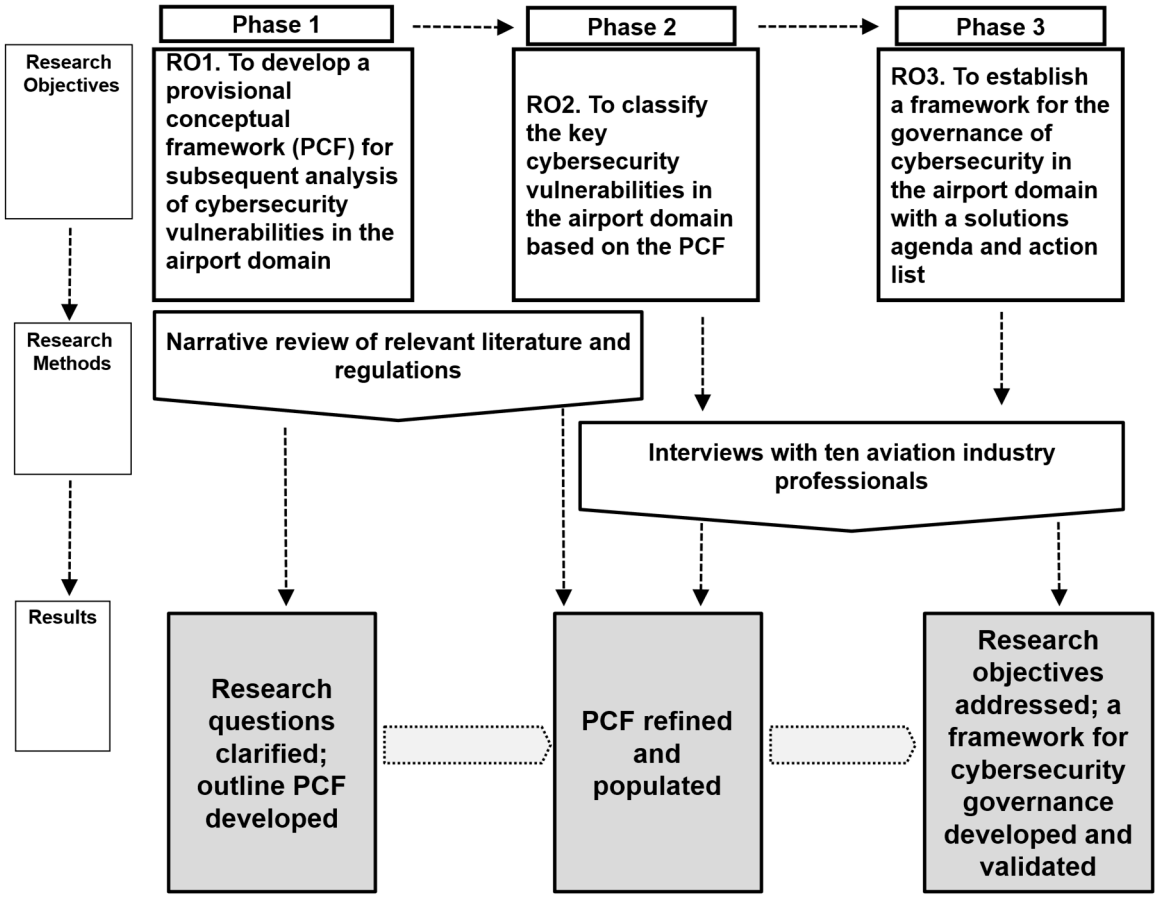

Figure 1. The three-phase research process.

In Phase 2, a questionnaire was developed based on the PCF and the issues that surfaced in the literature review. This was emailed to ten senior management practitioners in the airport industry and was followed up by semi-structured interviews. The questionnaire was divided into two parts: in the first, respondents were asked to consider the key vulnerabilities and related issues that challenge cybersecurity in the airport domain; and in the second, they were asked to consider key solutions and actions, and strategic imperatives, that need to be adopted and pursued to enhance cybersecurity.

A purposive sampling strategy was used to select participants, ensuring a diverse range of experiences across different organizations in the aviation sector. The ten interviewees were actively involved in airport cybersecurity (Table 1) and were selected on a pragmatic basis to provide a range of experience and perspectives. Given that aviation cybersecurity governance requires the integration of technical, governance, and business perspectives, the interview pool was composed of high-caliber participants—including C-level executives (e.g., CISOs, VPs) and senior directors—as well as individuals with both technical and strategic experience (such as P4 and P7). The group comprises an equal number of representatives from both airlines and airport operators, deliberately balancing strategic (C-level) and operational (middle/lower management) viewpoints. This qualified and senior sample ensured that, even with only 10 participants, a robust and actionable operational framework for aviation cybersecurity governance could be developed. Variety was provided in that the organizations were from different sectors, geographical areas, or enterprise types within the airport domain.

Table 1. Demographic and professional profile of interview participants.

Interviewee	Experience (yrs)	Age	Gender	Role/Position	Organization
P1	3	26	Female	Air Traffic Control/Electronics Engineer	General Directorate of State Airports Authority
P2	3	37	Male	IT Infrastructure & Operations Senior Manager	Airline Company
P3	17	45	Male	Information Security and Compliance Lead Analyst	Airline Company
P4	18	43	Male	Cyber Security Manager	Airline Company
P5	20	38	Male	Chief Information Security Officer	Airport Company
P6	28	50	Female	IT and Automation Director	Airport Company
P7	25	49	Male	VP of Information Technology	Airline Company
P8	5	35	Female	Senior Information Security Engineer	Airline Company
P9	26	49	Male	Information Security and Business Continuity Manager	Airport Company
P10	22	50	Male	Chief Information Security Officer	Airport Company

More specifically, the participant pool includes senior professionals from two major Turkish airline companies, three international/regional airport operators (including multiple airports across Türkiye, Europe, and the Middle East), a Turkish flag carrier, and a Gulf-based international airline operator. Geographically, organizations are represented in Istanbul, Ankara, and Antalya and have international operations in Saudi Arabia, Ireland, and beyond, ensuring coverage of diverse regulatory, operational, and infrastructural environments within the aviation ecosystem. At the validation step, in addition to a subset of the current interviewees, a cybersecurity manager from the United Kingdom Airports reviewed, validated, and provided feedback regarding the presented framework.

Anonymity of organization and respondent names was assured. The interviews were conducted in December 2024. Interviewees were presented with the outline PCF and asked their views on problem issues, possible solutions, and the required actions. Questions were asked in English, with each interview lasting 40 to 60 min. Interviews were conducted virtually via Microsoft Teams; informed consent was obtained prior to recording, and all sessions were transcribed verbatim for analysis. The initial focus in the analysis was on identifying the key vulnerabilities highlighted in the literature and reinforced through the interviews.

In Phase 3, this framework was further refined to evaluate the governance measures and compliance issues necessary to address these vulnerabilities. The analysis of the interview data informed the organization of governance and compliance actions, which are directly based on the insights of practitioners. In both phases, thematic analysis was used to analyze the interview data, following Braun and Clarke's [19] six-step framework to ensure methodological transparency and a robust audit trail. First, the authors read the interview transcripts from all ten senior practitioners (P1–P10) several times to ensure deep familiarity with the dataset. Subsequently, relevant segments were coded using descriptive and semantic labels (e.g., [Windows XP in use], [Vendor as weakest link]). Third, these initial codes were grouped into broader sub-theme categories, reflecting the technology, people-related, and organizational dimensions evidenced in the PCF, with

specific inductive sub-themes such as "weak management structure" and "uncontrolled social media usage" that emerged directly from the data. In the fourth step, the themes were iteratively reviewed and refined to ensure internal coherence and a clear distinction between themes, while also integrating supporting evidence from the literature review. Fifth, themes and sub-themes were defined, named, and linked to illustrative quotations that reflect sector-specific dilemmas, such as the "Availability vs. Security" trade-off. Finally, in the sixth step, the themes and sub-themes were integrated into the PCF to present an operational framework, connecting practitioner insights with the governance-oriented solution agenda. The thematic hierarchy, participant mapping, and representative quotes are detailed in Section 3.2 below.

Once the framework was developed, a validation exercise was undertaken involving 5 of the original interviewees (P1, P2, P5, P8, P10), randomly selected, and two further senior practitioners (P11: A senior cybersecurity manager from United Kingdom Airports; P12: Information Security Governance, Compliance & Internal Control Expert, Turkish Airlines Technology). These participants were sent a questionnaire containing the main research findings, plus 7 statements, requesting their assessment (from Strongly Agree to Strongly Disagree on a 5-point Likert scale). Participants were also asked to make additional comments as appropriate.

3. Results

This section addresses the three ROs. First, the PCF is set out, which is derived from an analysis of relevant literature. This is then used in conjunction with the analysis of the practitioner interviews to address ROs 2 and 3.

3.1. RO1: To Develop a Provisional Conceptual Framework (PCF) for Subsequent Analysis of Cybersecurity Vulnerabilities in the Airport Domain

In the wider context of IT systems, Heeks [20] set out four main dimensions of change that have been adopted by many IT studies—technology, people, process and structure. This is closely aligned with the human–organization–technology (HOT) framework put forward by Clegg et al. [21] in their study of IT performance, which was subsequently applied by Yusof et al. [22] in their analysis of systems-related errors in healthcare. As regards cybersecurity, a recent study [23] of measures adopted in private sector companies identified five change dimensions—financial, technological, human, external and organizational. More specifically, in the context of the airport domain, various authors and authorities have proposed concepts and frameworks for assessing cybersecurity vulnerabilities. PA Consulting Group, as reported by Hill [24], identified seven key trends that impact the aviation ecosystem as a whole: increased technology usage, hyper-connectivity, data-sharing obligations, customer centricity, IT/IoT towers, remote towers, and airports as mega-hubs. The Qatar Civil Aviation Authority (QCAA) [25] suggested intelligence gathering and sharing, people and process controls, technical controls, cyber insurance and supply chain management as key areas for cybersecurity development and management.

From these and other sources, technological aspects, people-related factors, and organizational issues emerge as common themes that can support a classification of vulnerabilities in the airport domain. There are multiple technology-related aspects of relevance, but the people factors (particularly human error) often constitute the weakest link in the entire cybersecurity chain for any information systems ecosystem [26]. Organization vulnerabilities within the airport domain include weaknesses within the management structures and related operational procedures that can be exploited, leading to potential security incidents. Organizational process inefficiencies and poorly documented or ambiguous procedures can also negatively impact cybersecurity.

At the same time, the principles embodied in the Governance, Risk and Compliance (GRC) approach to organizational risk and security management resonated with some of the change dimensions noted above [27]. The term "GRC" was first put forward by the Open Compliance and Ethics Group (OCEG) in 2007 as an organizational strategy to manage governance and risk whilst at the same time ensuring compliance with industry and government regulations. Of these three concepts, governance ensures a holistic, multi-faceted approach by establishing policies and procedures that balance technical advancements, human factors, and regulatory coherence. It also involves collaboration among stakeholders, including regulatory bodies and technology providers, to fortify the sector against cyber threats. Risk management supports the shift from reactive to proactive cybersecurity by identifying, assessing, and mitigating risks through robust technological defence mechanisms and a culture of cybersecurity awareness and education at all workforce levels. Finally, compliance emphasizes the need for international cooperation and standardized cybersecurity protocols, ensuring that security measures meet global regulatory requirements and contribute to a unified defence against cyber threats. This approach was deemed of relevance to the overall research aim and seen as a viable framework for classifying the research findings. The GRC approach is therefore combined here with technological, people-related and organizational dimensions for an analysis of the literature and interview findings. This is depicted in Figure 2 as the PCF for addressing RO2 and RO3.

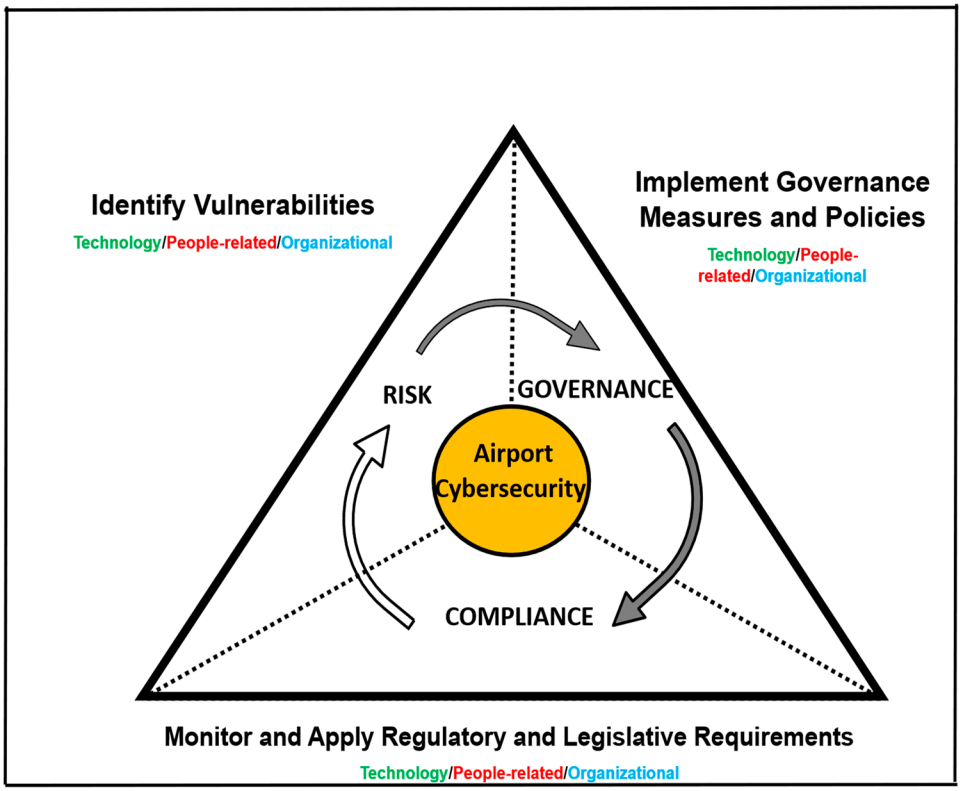

Figure 2. The provisional conceptual framework (outline model).

First risk factors as evidenced in the vulnerabilities and potential negative impacts in the airport domain were identified from the interview transcripts and cross-referenced with evidence from the literature (RO2). Governance, as a formal management system to address these identified risks, was then assessed in the light of interview findings and supporting literature. Compliance issues were analysed and reported to provide a structured pathway to adhere to legal, regulatory, and ethical obligations. By first classifying the vulnerabilities and then applying a comprehensive governance framework,

the GRC approach offers a holistic and actionable strategy for the responsible management of cybersecurity vulnerabilities in the airport domain (RO3).

3.2. RO2: To Classify the Key Cybersecurity Vulnerabilities in the Airport Domain Based on the PCF

The vulnerabilities and related risks in the airport domain are classified below in terms of technology issues, people-related and organizational factors as set out in the PCF above. This analysis draws upon both the extant literature and interview evidence (Table 2). The enhancement of the PCF, indicating the main vulnerabilities, is shown in Figure 3.

Table 2. Cybersecurity vulnerabilities in the airport domain: evidence from practitioner interviews.

Dimension	Sub-Theme	Initial Codes (Analytical Segments)	Synthesis	Interviewees	Representative Interview Quotations
Technology	Legacy IT/OT weaknesses	Outdated hardware; Protocols built 50 years ago; Lack of patch support; Windows XP machines.	Decades-old IT and OT platforms (e.g., baggage SCADA, avionics) cannot support modern security controls and remain unpatched.	P2, P3, P5, P6, P8, P10	"Some airports still run systems on Windows XP machines."—P6 "There are protocols running in operators, built like 40–50 years ago. Still, text-based protocols are running…"—P2
	API & web-application exposure	API security criticality; Bot-driven attacks; Web application vulnerability; Millions of daily users.	Public APIs serving millions of users become prime bot-driven attack vectors without mature authentication & monitoring.	P7	"Millions of users connect through web applications and APIs daily."—P7 "Microservices and the environments where APIs are hosted…must be protected."—P7
	Cloud services shortcomings (data-localisation constraints)	Data localization laws; Domestic hosting mandates; Sovereignty constraints.	National data-localisation laws block adoption of secure cloud platforms, forcing on-prem legacy stacks.	P6, P7	"Regulations keep data within the country, impacting the use of cloud services."—P7 Cloud computing—airports are not allowed as 'critical infrastructure'—must be hosted in Turkey."—P6
	Emerging technology (AI/IoT) attack-surface growth	Aviation 4.0 risks; Sensor proliferation; Zero-day threats in automation; Uncontrolled AI usage.	Rapid rollout of IoT sensors & AI workflows increases zero-day and supply-chain exposures that legacy controls cannot track.	P5, P7, P9, P10	"With new technologies like AI, there's a potential for more vulnerabilities."—P7 "Baggage handling system has many sensors—increases the threat surface area."—P9

Table 2. *Cont.*

Dimension	Sub-Theme	Initial Codes (Analytical Segments)	Synthesis	Interviewees	Representative Interview Quotations
Technology	Need for proactive security operations & testing	Penetration tests on all infrastructure; Vulnerability scanning; Red teaming exercises; Continuous monitoring.	The shift from reactive to proactive security through a continuous cycle of technical validation (e.g., penetration testing, red teaming) to identify and remediate infrastructure vulnerabilities before they can be exploited by adversaries.	P8, P9, P10	"...proactive threat modeling, using 'Red Team' and 'Purple Team' exercises to find vulnerabilities before they are exploited"—P8 "Conduct regular penetration testing, including red teaming exercises... to proactively find and fix vulnerabilities."—P10 "Penetration tests undertaken on all infrastructure... The agenda is built on a cycle of continuous security operations."—P9
	Insufficient Threat Intelligence & Information Sharing	Aviation cyber-threat-intelligence network; Sharing threat intelligence across ecosystem; Inadequate information sharing regarding incidents; Weak communication hindering sharing.	Besides existing cyber threat intelligent solutions, the imperative for a centralized, aviation-specific intelligence-sharing framework to overcome existing information asymmetry between stakeholders and enhance the collective defensive posture of the entire airport ecosystem.	P1, P3, P5, P8	"Aviation cyber-threat-intelligence network... information asymmetry in a hyper-connected industry is fatal."—P1 "Threat intelligence should be shared across the aviation ecosystem as a process improvement."—P3 "Lack of information shared about incidents involving airlines or third parties is a major gap."—P8

Table 2. *Cont.*

Dimension	Sub-Theme	Initial Codes (Analytical Segments)	Synthesis	Interviewees	Representative Interview Quotations
People-related	Poor cyber awareness levels (and phishing)	Tick-box training; Forgetting procedures; Phishing susceptibility.	Mandatory training is seen as a tick-box; staff, crew & management remain vulnerable to phishing & social engineering.	P2, P5, P6, P8, P10	"I believe the current cybersecurity awareness programs are not working well. They are just procedures that people forget in two hours."—P2 "Airport staff are vulnerable to spam emails, which can lead to computer compromises." —P8
	Skills shortage & retention	Salary competition; Loss of historical memory; Cyber-talent drain; Expertise gap.	Shortage of aviation-savvy cyber talent and high turnover undermine in-house security capability.	P4, P6, P2, P8, P9, P10	"It is difficult to find qualified cyber-security staff. . . a global problem."—P6 "I believe the current cybersecurity awareness programs are not working well. They are just procedures that people forget in two hours."—P2 "Airport staff are vulnerable to spam emails, which can lead to computer compromises." —P8
	Unregulated social media usage	Sharing badge cards online; Unauthorized duplication risk; Personal device leaks.	Sharing badge cards online, personal device comprimise risks, phising using social media	P5, P8	"Employees unknowingly expose security risks by sharing images of their badge cards on social media."—P5 "Crew's limited training on detecting phishing attempts; social media can be a cybersecurity risk."—P8

Table 2. *Cont.*

Dimension	Sub-Theme	Initial Codes (Analytical Segments)	Synthesis	Interviewees	Representative Interview Quotations
Organization	Uneven vendor/third-party security postures	Retail shops autonomy; Catering risks; Ecosystem maturity variance; Audit difficulty. Ground handling turnover; Contractor awareness gaps; Vendor as weakest link.	Hundreds of external entities with uneven security postures create back-door risk to airport core. Contractor staff lack security maturity, becoming the "weakest link". Breaches in vendor systems propagate into airport operations, amplifying impact.	P3, P4, P5, P6, P7, P8, P10	"Airports are ecosystems. . . suppliers are difficult to control."—P6 "A breach in any vendor can back door the airport's critical infrastructure."—P3 "Outsourced and third-party companies constitute risk. Need to be managed."—P4 "It recently changed actually. . . and it became the weakest link. Is the vendor right now?"—P3 "Suppliers are assessed. . . but difficult to control—e.g., cashier in Macdonalds."—P6
	Continuous service requirements (24 × 7 operations vs. security)	Availability over patching; Downtime pressure; Deferred maintenance window.	Continuous service requirements delay patching and slow incident response, prioritising uptime over security.	P2, P5, P8, P10	"In aviation, availability is very important. If a system goes down for two hours, thousands of passengers can be stuck."—P2 "Inability to apply security patches during flight operations."—P8 "Information security, cybersecurity-related risks should be considered the same as safety risks, as it can eventually affect people's lives."—P3 "Cybersecurity can be better if risks are evaluated very well. Managing risks effectively leads to solving problems effectively."—P8

Table 2. *Cont.*

Dimension	Sub-Theme	Initial Codes (Analytical Segments)	Synthesis	Interviewees	Representative Interview Quotations
Organization	Change management & procedural weaknesses	Bypassing procedures for speed; Inadequate CNS protocols; Non-standardized setups.	Weak change-management and missing certifications allow insecure updates and configurations.	P1, P2, P7, P8	"Importance of following procedures for technology updates."—P7 "In operations, time is very critical. . . they should not bypass procedures. Instead, they must follow the procedures."—P1 "Everyone acts differently across countries. . . lacking standards leads to workarounds." —P2
	Lack of corporate data ownership/ data governance deficit	Data classification deficit; Integration mapping gaps; Missing owner roles.	Missing data ownership, classification & integration mapping elevates systemic risk.	P3, P7	"Labeling data and understanding integrations is more vital than the cyber-security of the systems."—P7 "Missing data ownership, classification & integration mapping elevates systemic risk."—P3
	Reactive security posture	Bolting on security late; Old cultural behaviors; Post-incident investment.	Security bolted on after deployment; limited executive oversight leads to reactive culture.	P3, P5, P6	"Some old cultural behaviours and reactive approaches still exist."—P3 "Many organizations only invest in cybersecurity improvements after regulatory audits or security incidents."—P5

Table 2. *Cont.*

Dimension	Sub-Theme	Initial Codes (Analytical Segments)	Synthesis	Interviewees	Representative Interview Quotations
Organization	Overlapping & inconsistent regulations	Regulatory lag; Duplicate audits; Country maturity variance; Compliance fatigue. Global certification needs; Independent global audit; Sector-wide standardization.	Multiple national frameworks impose duplicate audits and conflicting controls.	P6, P8, P10	"Many overlaps within these regulations."—P8 "The maturity level of standards varies from country to country."—P10 "Independent audits are not conducted on suppliers. . . International standards must be complied with; establish independent audit organizations." —P1
	Weak management structure	Non-unified protocols; Disjointed response plans; Reporting line ambiguity.	Non-unified security processes between airlines, airport vendors, authorities; Disjointed response plans; Indirect reporting lines (Cyber operations to CIO)	P3, P6, P8, P10	"Multiple entities. . . working together without unified cybersecurity protocols. Disjointed incident response plans can lead to delays." —P10 "Strategic Imperative: Create centralized governance for cybersecurity to streamline efforts across stakeholders." —P10 "Governance must understand the business side requirements." —P8 "Cyber Security does not report directly to CIO but dotted line to IT/CIO."—P3

Table 2. *Cont.*

Dimension	Sub-Theme	Initial Codes (Analytical Segments)	Synthesis	Interviewees	Representative Interview Quotations
Organization	Lack of AI governance & defensive integration	Trusted AI environments; Controlled AI usage; AI-driven threat detection; AI-enhanced attack resilience; Regulatory lag regarding AI.	Establishing a strategic framework to manage the dual-nature of Artificial Intelligence in aviation; focusing on controlled deployment within trusted environments to mitigate new vulnerabilities while leveraging AI-driven analytics for advanced threat detection and defensive automation.	P1, P3, P4, P5, P7, P8, P10	"AI is used, but closely controlled. Using AI in uncontrolled, open-source environments may introduce new vulnerabilities." —P4 "With new technologies like AI, there's a potential for more vulnerabilities to be found. . . alongside the possibility of AI helping to patch them."—P7 "Continuous and intelligent sophisticated attacks with AI and automations. . . airport operating processes."—P10

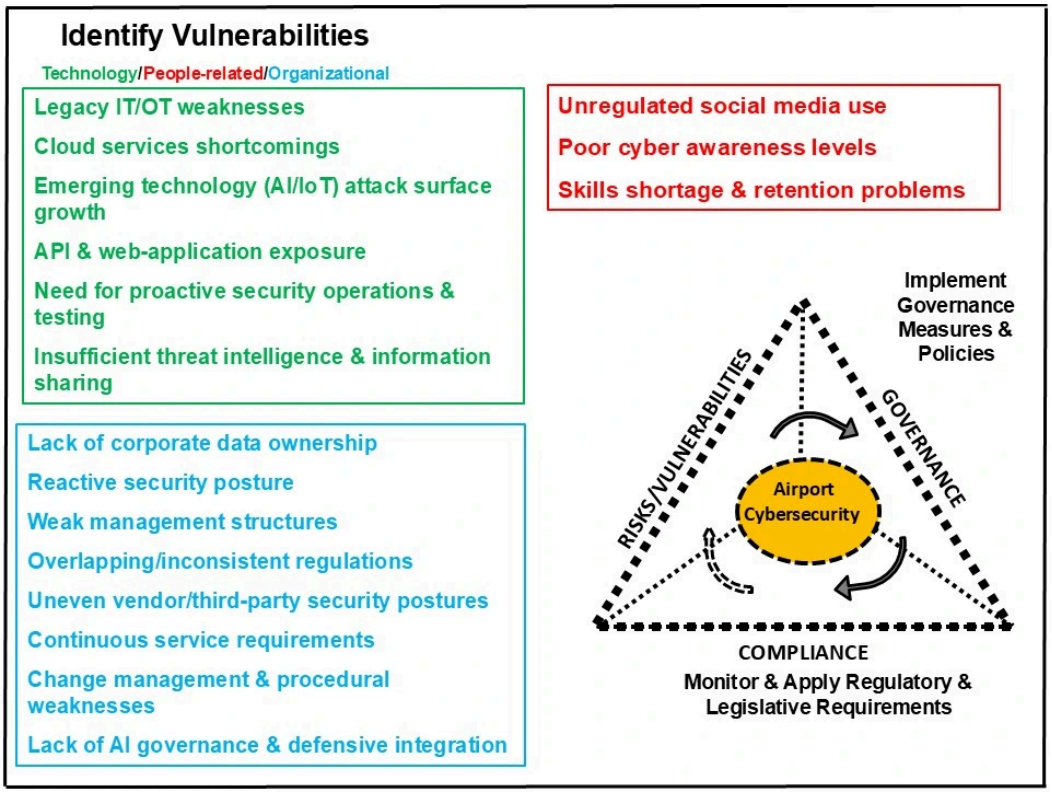

Figure 3. Key cybersecurity vulnerabilities in the airport domain.

3.2.1. Technology Dimension

Technology vulnerabilities in the airport domain are extensively discussed in the literature, which emphasizes that both the basic IT information systems and infrastructure, and the range of applications and add-on systems that rely in part on this basic infrastructure, are potentially vulnerable to cyberattacks. Network connectivity in airports may be prone to cyberattacks, and network designs that incorporate predefined cybersecurity requirements are of critical importance [25]. Murphy et al. [28] also highlights the risk of misconfiguration of the intrusion and malware detection systems and firewalls, and insufficiencies in Wi-Fi security measures.

Spaniel and Eftekhari [29] researched several airport cybersecurity attack scenarios and the vulnerabilities of the systems used in airports that are likely to be targeted by those criminals. Avionics software, baggage handling systems and smart devices used in airports, and systems connected to ground operations such as de-icing systems, aircraft tugs, and heating, ventilation and air conditioning (HVAC) systems, etc., were all examined in terms of the vulnerabilities that these systems may possess. In addition, airline operational systems for reservations, departure control, flight planning, and cargo operations can also be included. Goudge [30] reported that all these applications counted among the vulnerability points for airline operations, being targets for DDoS and spoofing attacks, thereby creating security and data privacy concerns.

Amongst the interviewees, a dominant perspective was the vulnerability of legacy IT and OT (operational technology) platforms. Six of the ten practitioners (P2, P3, P5, P6, P8, P10) described critical assets running on operating systems as old as Windows XP or on vendor-locked avionics that have never been patched. Because certification cycles are slow and upgrade paths uncertain, these platforms cannot accommodate modern controls such as full-disk encryption or zero-trust segmentation.

As the digital systems used in airports increase in complexity, and the number of smart devices used by passengers and employees grows, so aviation cyber-security is challenged in new ways and through new pathways [31]. The prevalence of cloud-based services constitutes a further risk, as does fog computing, which brings processing power and data storage closer to the physical infrastructure (such as IoT devices) [32]. Cloud-based services and fog computing rely on the internet, and thus data transferred between airport information systems and the cloud providers' servers may be exposed to third party intrusion. In addition, there are constraints on data localization in which laws block adoption of secure cloud platforms, forcing on-premises legacy stacks.

Whilst the adoption of IoT technologies in smart airports may significantly enhance operational efficiency and control through real-time monitoring, it also escalates the cyber threat landscape. By enlarging the attack surface, critical systems are more vulnerable to sophisticated cyber threats like Advanced Persistent Threats (APTs), emanating from inherent vulnerabilities in both hardware and software [33]. Indeed, some of the interviewees expressed concern that the rapid growth of IoT and AI workloads means that the technology surface is expanding faster than governance can follow. The exposure of public APIs and web services, and the constraints imposed by national data-localisation rules, were amongst the issues highlighted. P7 summarised the dilemma succinctly: "Millions of users connect through web APIs every day; we have no way to monitor the volume of bot traffic".

3.2.2. People Dimension

In the context of people-related factors impacting airport cybersecurity, social engineering activities that target employees and managers, insufficiently designed personal device (BYOD) policies, unregulated use of social media in the workplace, and malicious insiders are considered to be the main sources of vulnerabilities related to human operators. Such weaknesses can result in the proliferation of misinformation, viruses and malware. More specifically, in the airport domain, the lack of cyber awareness of airport personnel and operators constitutes a significant challenge for the industry in achieving higher security standards. At the same time, the shortage of basic technical skills and insufficient comprehension of the cybersecurity landscape exacerbate the problem. ENISA [34] reported that the constant increase in interconnectivity and interdependence of devices and systems was the main cause of human related cybersecurity vulnerabilities. The need for educating personnel and passengers was emphasised as a critical step in achieving the necessary level of cybersecurity.

This was emphasized by the practitioner interviewees. Five interviewees (P2, P5, P6, P8 and P10) judged security-awareness training programs to be inadequate; compulsory e-learning is "quickly forgotten" and phishing simulations still catch out both frontline and managerial staff. Maintaining effective cybersecurity processes and procedures requires appropriate staff training on best cybersecurity practice. The absence of such training can lead to increased susceptibility to social engineering attacks, phishing, or inadvertent introduction of malware [35].

A related issue raised in the interviews was the acute shortage of aviation-savvy cybersecurity professionals. Six respondents (P4, P6, P7, P8, P9, P10) reported problems recruiting or retaining talent, noting that engineers with deep OT expertise are lured away by better-resourced industries. This shortage not only slows remediation but also forces airports to rely on external integrators whose own personnel may be under-trained, creating a third human-centric risk: vendor staff as the new "weakest link" (P3). The 2023 Airport Cybersecurity Insights report [36] concludes that one of the major challenges is retaining and recruiting IT staff, emphasizing the need to find, train, and retain quality personnel, transform organizational digital culture, and implement measures to prevent and mitigate cyber threats. The risks involved in using outsourcing agencies and personnel are evident, although the experience and aviation knowledge of these external service providers can be of value from a security viewpoint. On balance, a lack of in-house knowledge and understanding is likely to increase vulnerability to cyber threats.

3.2.3. Organization Dimension

Organizational issues that impact the airport domain include weaknesses within the management structures and related operational procedures that can be exploited, leading to potential security incidents. There are several aspects here. Firstly, inadequate risk management occurs when there is a failure to properly identify, assess, and mitigate risks associated with cybersecurity threats to aviation systems. One interviewee depicted the airport as an "uncontrollable ecosystem" in which hundreds of suppliers, concessionaires and ground-handling agents operate semi-autonomously. Two-thirds of the interviewees (P3, P5, P6, P7, P8, P10) argued that uneven vendor security postures open back-door pathways into mission-critical systems. Third-party supply-chain exposure was raised as a key issue by five practitioners (P3, P5, P6, P8, P10), who warned that a breach in a passenger-service system, flight-information display, or catering partner could propagate laterally and compromise airport command centres within minutes.

A more specific concern raised by interviewees was the lack of corporate data ownership and the implications for data integrity. Two respondents (P3, P7) raised this point

explicitly, both arguing that without clear data ownership, classification and architectural mapping, even well-engineered controls can be circumvented. A broader concern is the reactive posture that still dominates policies and metrics development and implementation, with these measures often being appended after systems are deployed, reflecting what P3 called "old cultural behaviours".

A further organizational issue raised in the interviews is the knock-on implications of the industry's mandate for uninterrupted, twenty-four-hour operations. Because a two-hour outage can strand thousands of passengers, patch windows are continually deferred and incident-response decisions become markedly conservative. In three interviews (P5, P8, P10), the inability to reboot, even after severity-one alerts, was cited as a habitual trade-off. In addition, procedural discipline is uneven: one expert (P7) linked several recent misconfigurations to weak change-management controls rather than to purely technical faults.

Poor communication across the airport organization may impede threat intelligence sharing and collaborative response efforts. This reflects the lack of a multi-stakeholder model at the international level for cybersecurity-related issues [37]. In this context, ECCSA [9] advises that effective communication with both internal and external stakeholders is essential to achieve a sufficient level of information security awareness, highlighting the importance of comprehensive stakeholder engagement in enhancing the overall cybersecurity posture within the aviation sector. Finally, compliance with national, international, and sectoral regulations and standards, such as those of the EU, Federal Aviation Administration (FAA) [28], and ICAO, is an important aspect in maintaining required cybersecurity levels at organization level.

In terms of data privacy and security, three of the interviewees (P6, P8 and P10) pointed to overlapping aviation frameworks that impose duplicate audits and sometimes contradictory control expectations. The resulting patchwork forces security teams to work simultaneously under GDPR, ISO/IEC 27001, local data-retention mandates and evolving sector guidance, stretching limited staff even further.

In summary, an analysis of the relevant literature and interviewee feedback captured a systemic picture in which legacy technology, human limitations and organizational complexity intersect with patchy governance, escalating risk and fragmented compliance regimes. The prevalence counts shown in Table 2 show that no single vulnerability category stands alone; rather, weaknesses in one dimension amplify vulnerabilities in the others. This interdependence underscores the need for integrated mitigation strategies—technical upgrades paired with skills development, vendor-management reform and regulatory harmonisation—rather than piecemeal fixes aimed at individual symptoms. This is now developed further in response to RO3.

3.3. RO3: To Establish an Operational Framework for the Governance of Cybersecurity in the Airport Domain with an Associated Solutions Agenda

This section addresses RO3 and examines how governance and compliance initiatives can be utilized to mitigate risk by addressing the vulnerabilities identified above with a solution agenda based on interview evidence (Table 3). The enhancement of the PCF, providing a solution agenda, is also shown in Figure 4.

Table 3. Solution agenda for aviation cybersecurity governance.

Governance/Compliance Objective	Dimension	Concrete Actions to Mitigate Risk	Priority	Implementation Term	Interviewee Support
Secure the expanding digital surface	Technology	Defence-in-Depth modernisation: upgrade legacy HW/SW, robust encryption, continuous monitoring & resilient back-ups (P1); AI & Advanced Monitoring: Deploy API bot-mitigation, Zero-Trust controls, and AI-based SOC analytics (P5, P7, P8, P10); Proactive Testing: Conduct continuous penetration testing, vulnerability scanning, and Red/Purple Teaming exercises (P8, P9, P10)	Critical	Short to Medium Term	P1, P5, P6, P7, P8, P9, P10
Treat cyber risk as a flight-safety hazard	Technology/ Organisational	Integrate cyber scenarios into Safety Management System & run joint tabletops (P3, P7); continuous third-party risk scoring & right-to-audit (P6, P10).	High	Immediate/Ongoing	P3, P6, P7, P10
Institutionalize practical, role-specific training	People-related	Scenario-based drills & run-books (P1); micro-learning & phishing simulations (P2, P10); bonded scholarship/apprenticeship pipeline (P6, P8). Implement phishing simulations and awareness campaigns and policy regarding "uncontrolled social media usage" (P5, P8)	High	Immediate	P1, P2, P5, P6, P8, P10
Embed procedural discipline & 24 × 7-safe change	Organisational/ Technology/People-related	Specialised OT change-control procedures (P1); change windows tied to Safety Risk Matrix, patch rollback rehearsals (P5, P10); tier-1 SOC with safety-critical playbooks (P7, P8). OT Mindset Shift: Transition OT management from TCO focus to a full security lifecycle approach (P10)	Medium	Medium Term	P1, P5, P7, P8, P10
Elevate cyber governance & shared intelligence	Organisation/ Technology	Aviation Cyber Threat-Intelligence Network: Establish a sector-wide intelligence sharing network to eliminate information asymmetry (P1, P3, P5, P8); board-level Cyber Governance Council with safety-linked KPIs (P3, P6); data-integration inventory & owner assignment (P7). Unified Leadership: Establish a board-level Cyber Governance Council and address weak management structures by unifying disjointed protocols across stakeholders (P10); AI & Data Governance: Enforce trusted AI environments, formalize data ownership, and implement data classification (P4, P7)	Strategic	Medium to Long Term	P1, P3, P4, P5, P6, P7, P8, P10

Table 3. *Cont.*

Governance/Compliance Objective	Dimension	Concrete Actions to Mitigate Risk	Priority	Implementation Term	Interviewee Support
Modernize and harmonize oversight	Organisation	Update standards & create independent global audit bodies (P1); ICAO/EASA binding cyber-certifications (P7); recognise secure-cloud equivalence, streamline audits (P6, P8, P10).	Strategic	Long Term	P1, P6, P7, P8, P10

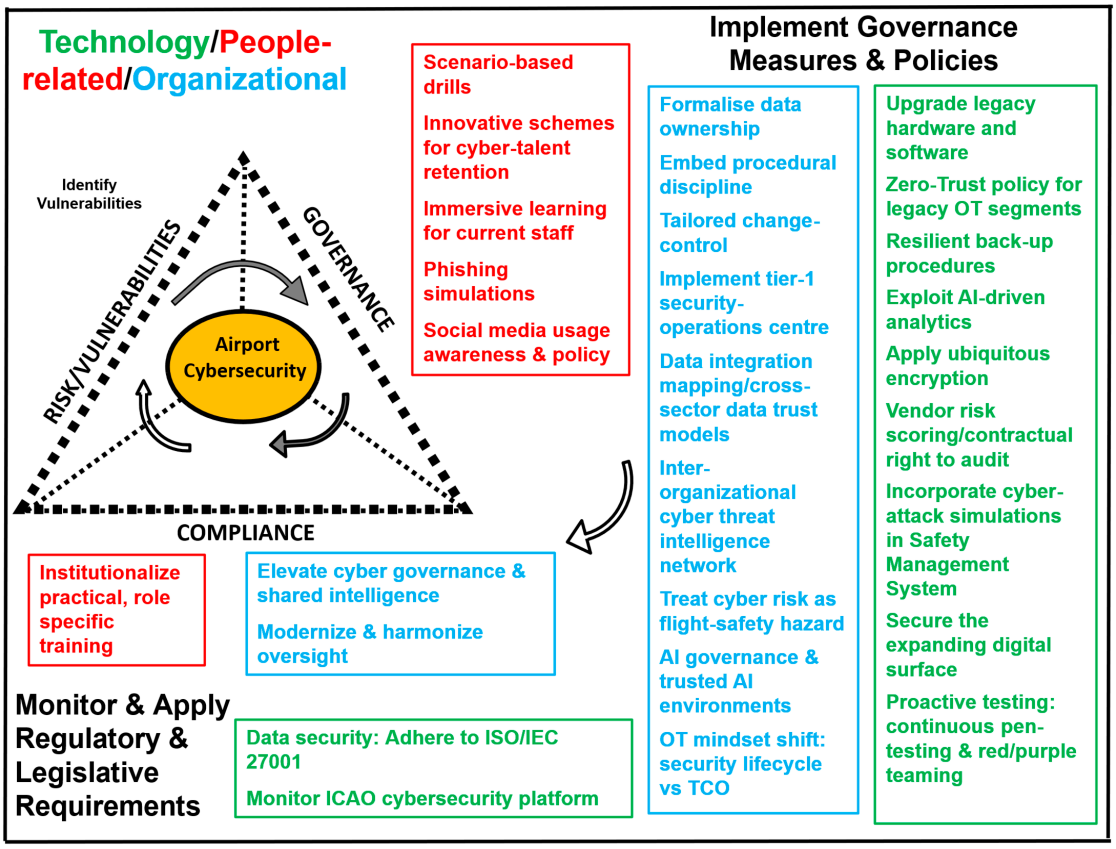

Figure 4. Aviation cybersecurity governance and compliance: key aspects, factors and issues.

3.3.1. Technology Dimension

The expanding digital surface in the airport domain constitutes a major technology management challenge. P1 frames the strategic baseline as a defence-in-depth modernisation programme: legacy hardware and software must be upgraded, encryption must be ubiquitous, and continuous monitoring as well as resilient back-ups are non-negotiable. P6, P7 and P10 reinforce this by calling for a Zero-Trust policy around legacy OT segments and specialised bot-mitigation at the API layer, while P5 and P8 add that AI-driven analytics are essential to cope with log volumes which no human team can review in real time. The convergence of these viewpoints shows that the sector regards technology renewal and granular perimeter control as inseparable parts of the same objective.

Some interviewees suggested measures to elevate the significance of ransomware or PLC-manipulation (control logic manipulation attack) scenarios. P3 and P7 suggested folding ransomware or PLC-manipulation scenarios into the Safety Management System and rehearsing them in joint table-top exercises. P7 asserted that "cyber security risks should be considered the same as safety risks". As regards third-party exposure, P6 and P10 recommend continuous vendor-risk scoring and insisting on a contractual right to

audit suppliers, thereby addressing third-party exposure. One implication here is that treating cyber events as safety hazards aligns them with existing operational doctrines and unlocks established funding and accountability mechanisms.

3.3.2. People-Related Dimension

P1 argues that conventional awareness presentations must give way to scenario-based drills that mirror time-critical air-traffic operations; this plea resonates with P2's frustration with "tick-box" training, and with P10's call for more phishing simulations. Both P6 and P8 cite the need for a bonded scholarship or apprenticeship pipeline to retain scarce cyber-talent, thereby tackling the recruitment problem identified above. The interviewees propose a blend of immersive learning for current staff and structural incentives for future staff, underscoring that awareness and talent retention are complementary, not alternative, remedies.

3.3.3. Organization Dimension

Organizational governance can be enhanced through the embedding of procedural discipline without jeopardising twenty-four-hour service continuity. P1 recommends tailoring change-control to OT and air-traffic systems rather than grafting generic ITIL-based solutions onto them. P5 and P10 elaborate on this by insisting that every patch window be linked to a Safety Risk Matrix and rehearsed with a rollback plan, while P7 and P8 see a tier-1 security-operations centre with safety-specific playbooks as the operational engine that makes such discipline reproducible. At the same time, choosing an effective risk assessment methodology is a necessary pre-requisite [38,39] to effectively managing cyber risk, as there are often different perceptions of cybersecurity risks, and airport management may interpret guidelines in different ways, resulting in inconsistencies in the application of cybersecurity practices in different airports [38]. Together these comments articulate a pragmatic path for reconciling availability imperatives with responsible change management. Other participants allude to the need for inter-organizational measures. P1, for example, calls for a sector-wide aviation cyber-threat-intelligence network, arguing that information asymmetry is fatal in a hyper-connected industry. P3 and P6 advocate a board-level cyber-governance council, whereas P7 highlights the need for a complete map of data integrations and formal data ownership. The thread running through these statements is that strategic awareness must be both shared horizontally across the sector and elevated vertically to senior leadership.

Compliance with national, international, and sectoral regulations and standards, is an important organizational aspect in maintaining required cybersecurity levels in the airport domain (see Appendix A). Data protection is one key aspect in this context, and the ISO/IEC 27001 standard [40] outlines guidelines to secure data. It ensures that only authorized people can access and update data and make it available when needed. In addition, since the early 2000s, ICAO has provided a platform for the international air transport community to collaborate on cybersecurity. This aims to foster a consistent, comprehensive, and unified approach that aligns with the priorities of civil aviation.

The significance of compliance is brought to the fore by regulatory fatigue and obsolescence. P1 urges an update of international standards together with independent global audit bodies. P6, P8 and P10 extend the argument to cloud adoption and duplicate audits, recommending mutual recognition frameworks to avoid redundant effort. These comments converge on the idea that regulation should be forward-looking, harmonised and outcome-based, reducing overheads while raising the security bar.

Evidence from the interviews shown in Table 3 and Figure 4, allied with literature analysis, suggests a coherent programme is required. Technological renewal must be

accompanied by skilled people and disciplined processes; governance and shared intelligence create the visibility required for risk-model integration; and modernised compliance provides the external incentives and benchmarks that sustain progress. Table 3 sets out a solutions agenda for practitioners working with the cybersecurity challenges of the airport domain. This builds upon the key governance issues identified above and the corresponding compliance actions. Six key objectives are distilled from the above analysis with concrete actions linked to each one. Because each initiative is underpinned by multiple independently voiced recommendations, the agenda captures practitioner consensus rather than individual preference, making it a defensible blueprint for sector-wide action. A priority ranking is provided, based on flight-safety impact. Specifically, "Critical" and "High" priorities are assigned to actions that mitigate immediate technical vulnerabilities or the "human link", while longer-term structural changes are categorized by their implementation timeframe and complexity. This allows practitioners to distinguish between "quick wins" and longer-term measures probably requiring more significant capital investment.

As a form of validation, the PCF (Figure 2), the final framework (Figure 5) and the solutions agenda (Table 3) were emailed (as part of a summary validation form) to five of the participants and to two additional experts, as noted above in Section 2. They were asked to study the project information and assess seven statements about these findings on a 5-point Likert scale. The results (Table 4), and the accompanying comments, indicate a strong agreement with the statements indicating a positive perception by participants. The only reservations came from P8, who gave a neutral assessment of statement 7 (Implementing the framework is feasible in typical airport operating conditions, and the framework provides sufficient guidance to prioritize actions over time) and from P11, who similarly gave a neutral view of statement 6 (The framework adequately covers key third-party and supply-chain dependencies that materially influence airport cybersecurity risk). Here P11 requested that Supply Chain Governance be added as an important governance and compliance measure. P1 also noted that "given that Internet Service Providers (ISPs) are a critical point of dependency for airport infrastructure and play a central role in elements such as cyber threat defense, line redundancy, and the transmission of cyber intelligence, it is considered beneficial to include ISPs under 'Supply Chain' or as a separate heading with a more specific emphasis".

P5 suggested that "focusing on 'Continuous Service' alone is no longer enough. It must shift to 'Cyber Resilience and Continuity'... It changes this strategy from trying to be 'unhackable' to being 'unbreakable' when faced with problems". P11 also suggested AI governance (including shadow AI) should be included as a further governance measure, citing the use of generative AI as "enabling highly convincing phishing campaigns" and the dangers of "unauthorized or unmonitored use of AI tools within organisations". P5 also suggested that "Mapping data integration is just a technical task. To truly secure our ecosystem, we need to expand this into Cross-Sector Data Trust Models...ensuring that data sharing is secure and compliant across different institutions". P8 highlighted the need for proactive threat modeling, using 'Red Team' and 'Purple Team' exercises to find vulnerabilities before they are exploited, and P10 similarly highlighted the need for regular penetration testing to proactively find and fix vulnerabilities. These suggestions have been incorporated into the final framework discussed below in Section 4. P5 summarised his perspective thus: "Airports are not ideal technology labs; they are complex operational environments with legacy systems and heavy reliance on outsourcing.... This framework acknowledges these real-world constraints as manageable risks rather than insurmountable obstacles".

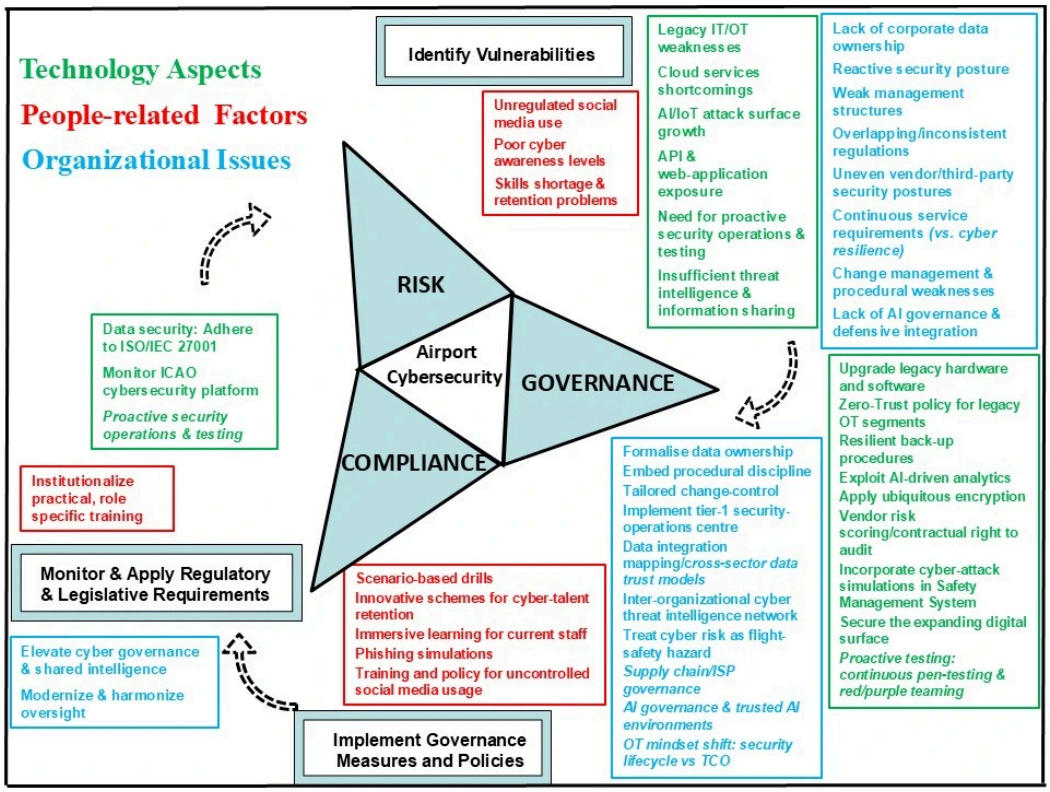

Figure 5. Aviation cybersecurity governance framework for the airport domain: summary figure (post validation enhancements are in italics).

Table 4. Findings validation: statement assessment by participants. (SA = Strongly Agree; A = Agree; N = Neutral; D = Disagree; SD = Strongly Disagree).

Statement	P1	P2	P5	P8	P10	P11	P12
1. Overall, the framework provides a realistic assessment of current cybersecurity vulnerabilities and related governance and compliance issues in the airport domain	SA	A	SA	A	A	A	SA
2. The Risk–Governance–Compliance perspective is appropriate for a comprehensive assessment of cybersecurity in the airport domain.	SA	SA	SA	A	A	SA	SA
3. The classification of issues around the three change dimensions of technology–process–people provides a logical basis for developing appropriate solutions.	SA	SA	SA	A	SA	A	SA
4. The framework can be used in practice as a guide to support the monitoring and analysis of cybersecurity issues in the airport domain.	SA	A	SA	A	SA	SA	SA
5. The governance objectives and concrete actions are clear, actionable and aligned with the operational framework.	SA	A	SA	A	A	A	SA
6. The framework adequately covers key third-party and supply-chain dependencies (e.g., airlines, ground handlers, OT vendors, regulators) that materially influence airport cybersecurity risk.	A	A	SA	A	A	N	SA
7. Implementing the framework is feasible in typical airport operating conditions (legacy OT, outsourcing, budget/skills constraints), and the framework provides sufficient guidance to prioritize actions over time	A	A	SA	N	A	SA	A

While the solutions agenda is primarily focused on technology and organizational issues, it also requires a set of people-related change management capabilities to be successfully implemented. These include:

A holistic, multi-faceted approach: to balance technical advancements, human factors, regulatory coherence, and international collaboration.

Collaborative efforts among stakeholders: the aviation industry is not an isolated entity but part of a broader ecosystem that includes regulatory bodies, technology providers, airline operators, and, importantly, the flying public. Each stakeholder plays a vital role in fortifying the sector against cyber threats.

A cultural shift towards cybersecurity awareness and education: the aviation industry's commitment to such strategies, coupled with a clear vision for future research to explore uncharted territories of cybersecurity, will not only enhance resilience but also ensure the sustained safety and trust in global air travel. A recent industry report [41] highlights the current low level of awareness of cybersecurity threats amongst industry staff.

A transition from reactive to proactive cybersecurity: This entails not only the implementation of robust technological defenses but also a clear vision for future research to explore uncharted territories of cybersecurity, which will not only enhance resilience but also ensure sustained safety and trust in global air travel.

International cooperation and standardised protocols: The interconnected nature of global aviation demands a harmonized approach to ensure that security measures are not just localised solutions but part of a global shield against cyber threats. In this context, the Airports Council International (ACI) has developed the Airport Excellence (APEX) in Cybersecurity Assessment program [42] to help airports of all sizes conduct a thorough evaluation of their cybersecurity environment [42]. This structured program can be aligned with established standards and regulatory frameworks, including ISO/IEC 27001:2022 [40], the CER Directive [43], the NIS 2 Directive [44], the Cyber Resilience Act [45], and ICAO cybersecurity culture guidance [46], ensuring both relevance and depth in its approach. At the same time, as cybersecurity becomes increasingly important in civil aviation, national authorities such as Türkiye and Qatar [25,47] have started to introduce their own sector-specific regulations and technical guidance. For instance, in Türkiye, the Directorate General of Civil Aviation has released the Instruction on Cybersecurity for Civil Aviation Enterprises [47]. This document outlines the cybersecurity requirements, organizational responsibilities, and incident response procedures for all licensed civil aviation operators [47]. The key aviation cybersecurity authorities, organizations, and regulatory instruments are outlined in Table A1.

4. Conclusions

This article builds upon previous research to develop and validate an overarching framework for the management of cybersecurity in the airport domain in the digital era (Figure 5). First the article pinpoints the key cybersecurity concerns shared by multiple stakeholders in the aviation sector. Second, research findings are used to evolve and validate a model based on Governance Risk and Compliance principles which can provide a viable framework for the future management of aviation cybersecurity. Third, the framework is validated via interviews with ten industry practitioners and expanded to provide a solutions agenda. It is imperative for airport organizations to continuously evaluate and adapt their cybersecurity strategies to address evolving threats. As the number of partners operating at airports to provide different services has increased, so the need for interconnectivity and interdependence of the systems, networks and applications, and data sharing between stakeholders has grown accordingly. Digital systems have become increasingly integrated into airport communication and management systems in recent years.

This has amplified the risk of cyberattacks, necessitating rigorous cybersecurity measures and frameworks, and the cybersecurity implications have become increasingly complex. This article synthesizes the key cybersecurity vulnerabilities in this environment and puts forward an overarching framework and solutions agenda for addressing these challenges.

At the same time, international regulations and agreements play a vital role in the standardization of cybersecurity practices in the airport domain and across the aviation industry as a whole. Carefully structured regulations and standards play a key role in achieving consistent and coherent implementation of cybersecurity practices across the air transportation industry on an international level. The lack of metrics and standards to measure the effectiveness of cybersecurity practices in the airport domain is an area that requires attention from authorities. An integrated global effort is required to strengthen the aviation sector, emphasizing the application of ICAO-recommended practices and aligning national regulations with international cybersecurity standards [11–13,46], as also highlighted in the literature [48].

A GRC-based cybersecurity governance framework for the airport domain, utilizing the PCF, is illustrated in Figure 5. This framework highlights technology, people-related and organizational elements, based on a continuous improvement cycle of identify, implement and monitor. A summary of key aspects, factors and issues is provided in Table 5.

Table 5. Vulnerabilities, governance and compliance: an identify–implement–monitor cycle (post-validation enhancements are in **bold**).

	Identify Vulnerabilities	**Implement Governance Measures & Policies**	**Monitor & Apply Regulatory & Legislative Requirements**
Technology Aspects	Legacy IT/OT weaknesses Cloud services shortcomings AI/IoT attack surface growth API & web-application exposure **Need for Proactive Security Operations & Testing** **Insufficient Threat Intelligence & Information Sharing**	Upgrade legacy hardware and software Zero-Trust policy for legacy OT segments Resilient back-up procedures Exploit AI-driven analytics Apply ubiquitous encryption Vendor risk scoring/contractual right to audit Incorporate cyberattacks simulations in safety management system Secure the expanding digital surface **Continuous Proactive Testing (Red/Purple Teaming)**	Data security: Adhere to ISO/IEC 27001 Monitor ICAO cybersecurity platform Proactive Security Operations & Testing
People-related Factors	Unregulated social media use Poor cyber awareness levels Skills shortage & retention problems	Scenario-based drills Innovative schemes for cyber-talent retention Immersive learning for current staff Phishing simulations **Policy for uncontrolled social media usage**	Institutionalize practical, role specific training
Organizational Issues	Lack of corporate data ownership Reactive security posture Weak management structures Overlapping/inconsistent regulations Uneven vendor/third-party security postures Continuous service requirements (vs. cyber resilience) Change management & procedural weaknesses **Lack of AI Governance & Defensive Integration** **Budget-driven (TCO) vs. Security-driven mindset**	Formalize data ownership Embed procedural discipline Tailored change-control Implement tier-1 security-operations centre Data integration mapping/cross-sector data trust models Inter-organizational cyber-threat-intelligence network Treat cyber risk as flight-safety hazard Supply chain/ISP governance **AI Governance & Trusted AI environments** **OT Mindset Shift (Security Lifecycle focus)**	Elevate cyber governance & shared intelligence Modernize & harmonize oversight

This study has its limitations, as it relies on secondary sources and evidence from ten industry professionals. Given the relatively small sample size, the potential for social-desirability bias was critically assessed, notably because participants held senior roles that might encourage overly positive reporting. To assess this, brief notes were taken after each interview, and the responses from individuals in different roles were compared to determine if anyone was providing overly positive answers. In fact, instead of emphasizing compliance, interviewees spoke frankly about, for example, unpatched Windows XP machines, deferred patching during 24/7 operations, and an "uncontrollable" vendor ecosystem, suggesting minimal desirability distortion. Regarding interview language, English was chosen because cybersecurity terminology is largely English-based and all interviewees work in English-speaking technical environments. However, it is acknowledged that certain cultural or idiomatic nuances may have been lost during the interviews, but the authors believe the findings provide a sound basis for further research and can act as an effective framework for conceptualizing and managing a wide array of cybersecurity issues in a rapidly evolving technology environment.

Such research could advance this field of investigation by further developing the GRC framework proposition in specific areas of the aviation ecosystem. Individual airports and operators could be studied and analyzed, and the perspectives of different stakeholders assessed through further primary interviews. This may provide further inductive development of the framework and solutions agenda presented here, which could also be extended to include the aircraft and air traffic control domains. However, cybersecurity in the airport domain alone remains a problematic of ever widening scope, rapidly evolving in its manifestation, and with many moving parts. It is hoped this article has been of some value in charting the current status quo and in providing a framework of value to practitioners and other researchers in this field of study.

Author Contributions: Conceptualization, B.M. and H.B.D.; methodology, B.M., H.B.D. and M.W.; validation, B.M., H.B.D. and M.W.; formal analysis, B.M., H.B.D. and M.W.; investigation, B.M., H.B.D. and M.W.; data curation, B.M., H.B.D. and M.W.; writing—original draft preparation, B.M., H.B.D. and M.W.; writing—review and editing, B.M. and M.W.; visualization, B.M., H.B.D. and M.W.; supervision, B.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study was conducted in accordance with applicable ethical principles and the institutional guidelines of Boğaziçi University, Turkey. The research protocol for the project titled "Towards a Human Organization Technology and Governance Risk Compliance based Aviation Cybersecurity Framework", upon which this article is based, was reviewed and approved by the Boğaziçi University Social Sciences and Humanities Human Research Ethics Committee (SBINAREK) at its 2025/06 board meeting on 28 July 2025 (application number: 2025-54; document number: E-84391427-050.04-249967, dated 11 September 2025).

Informed Consent Statement: All participants provided informed consent prior to the interviews, and confidentiality and the protection of personal data were strictly ensured. In accordance with the approved ethical protocol, all identifiable interview data will be permanently deleted after publication of the study.

Data Availability Statement: Due to confidentiality and ethical considerations regarding interview-based qualitative data, as well as the sensitive nature of aviation cybersecurity, the datasets generated and analyzed in this study are not publicly available. These data are securely stored within a university environment. De-identified excerpts may be requested from the corresponding author, subject to reasonable requests and institutional approval.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Civil Aviation Cybersecurity Landscape: Authorities and Industry Organizations, and Regulatory Instruments

Table A1. Main civil aviation authorities, organizations, and regulatory instruments referenced in the text.

Related References	Authority/Agency/Institute	Standard/Regulation/Act/Document	Subject Area
[37]	IATA (International Air Transport Association)	Air Transport Security	Airlines
[28]	FAA (Federal Aviation Administration) Transportation Research Board	Airport Cooperative Research Program	US-based airlines and airports
[10]	Société Internationale de Télécommunications Aéronautiques (SITA):	Air Transport IT Insights	Airlines and Airports
[43–45]	EU	Directive on the Resilience of Critical Entities Network and Information Systems Directive 2 Cyber Resilience Act	EU member states
[9]	European Centre for Cybersecurity in Aviation (ECCSA) of the European Union Aviation Safety Agency (EASA)	Easy Access Rules for Information Security	Companies, Organizations, and Institutions in EASA Member States
[15]	UK Civil Aviation Authority (UKCAA)	Cyber Security Oversight Process for Aviation	UK airlines and airports
[11–13,46]	ICAO (International Civil Aviation Organization)	Aviation Cybersecurity Strategy Cybersecurity Policy Guidance Cybersecurity Culture	Countries
[40]	International Standards Organization	ISO/IEC 27001:2022 Information Security Management Standard	Countries
[34]	ENISA (the European Union Agency for Cybersecurity)	Securing Smart Airports	EU member states
[47]	Turkish Directorate General of Civil Aviation	Instruction on Cybersecurity for Civil Aviation Enterprises (SHT-SİBER, 2022)	Airlines, airports, and Air Traffic Control services in Türkiye
[25]	Qatar Civil Aviation Authority	Aviation Cyber Security Guidelines	Airlines, airports, and Air Traffic Control systems in Qatar
[42]	Airports Council International (ACI)	Airport Excellence (APEX) in Cybersecurity Assessment Program	Airports (cybersecurity assessment; airports of all sizes)

References

1. Leśnikowski, W. Threats from Cyberspace for Civil Aviation. *Wiedza Obron.* **2021**, *276*, 124–153. [CrossRef]
2. Cooper, P. *Aviation Cybersecurity: Finding Lift, Minimizing Drag*; Atlantic Council, Brent Scowcroft Center on International Security: Washington, DC, USA, 2017.
3. Mrežar, M. PNR Agreements and Related Cybersecurity Risks. Master's Thesis, University of Zagreb, Zagreb, Croatia, 2023; pp. 34–38.
4. Żmigrodzka, M. Cybersecurity—One of the Greatest Challenges for Civil Aviation in the 21st Century. *Saf. Def.* **2020**, *6*, 33–41. [CrossRef]

5. Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information* **2022**, *13*, 146. [CrossRef]
6. Janson, M. Enhancing Cyberspace Monitoring in the United States Aviation Industry: A Multi-Layered Approach for Addressing Emerging Threats. Doctoral Dissertation, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA, 2023.
7. Hilderman, V. Why Aviation Needs to Prioritise Cybersecurity. Airport World. 2023. Available online: https://airport-world.com/why-aviation-needs-to-prioritise-cybersecurity/ (accessed on 20 April 2025).
8. Grygorov, O.; Basysta, A.; Yedeliev, R.; Paziuk, A.; Tropin, Z. International Cyber Security Strategy as a Tool for Comprehensive Security Assurance of Civil Aviation Security: Methodological Considerations. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 332–337.
9. European Centre for Cybersecurity in Aviation (ECCSA). Easy Access Rules for Information Security. 2023. Available online: https://www.easa.europa.eu/en/document-library/easy-access-rules/first-easy-access-rules-information-security-regulations-eu (accessed on 27 May 2025).
10. SITA. 2018 Air Transport Cybersecurity Insights. SITA. 2018. Available online: https://www.sita.aero/resources/surveys-reports/air-transport-cybersecurity-insights-2018/ (accessed on 27 May 2025).
11. ICAO. Cybersecurity Action Plan. 2022. Available online: https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx (accessed on 9 April 2024).
12. ICAO. Aviation Cybersecurity Strategy. 2019. Available online: https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx (accessed on 9 April 2025).
13. ICAO. Cybersecurity Policy Guidance. 2022. Available online: https://www2023.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf (accessed on 9 April 2025).
14. UK Civil Aviation Authority. Policy, Oversight, Strategy, Regulations. 2018. Available online: https://www.caa.co.uk/commercial-industry/cyber-security/ (accessed on 27 May 2025).
15. UK Civil Aviation Authority CAP1753. Cyber Security Oversight Process for Aviation. 2024. Available online: https://www.caa.co.uk/our-work/publications/documents/content/cap1753/ (accessed on 27 May 2025).
16. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [CrossRef]
17. Bell, E.; Harley, B.; Bryman, A. *Business Research Methods*, 6th ed.; Oxford University Press: Oxford, UK, 2022.
18. de-Miguel-Molina, B.; de-Miguel-Molina, M.; Albors, J. How to undertake a literature review through bibliometrics. An example with review about user innovation. In *1st International Conference on Business Management*; Universitat Politècnica de València: Valencia, Spain, 2015. Available online: https://www.semanticscholar.org/paper/How-undertake-a-literature-review-through-An-with-de-Miguel-Molina-de-Miguel-Molina/4954253df6065920aa633275cf6ae89d091405c1 (accessed on 8 May 2025).
19. Braun, V.; Clarke, V. Using thematic analysis in psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [CrossRef]
20. Heeks, R. Information Systems and Developing Countries: Failure, Success, and Local Improvisations. *Inf. Soc.* **2002**, *18*, 101–112. [CrossRef]
21. Clegg, C.; Axtell, C.; Damodaran, L.; Farbey, B.; Hull, R.; Lloyd-Jones, R.; Nicholls, J.; Sell, R.; Tomlinson, C. Information technology: A study of performance and the role of human and organizational factors. *Ergonomics* **1997**, *40*, 851–871. [CrossRef]
22. Yusof, M.; Takeda, T.; Shima, Y.; Mihara, N.; Matsumura, Y. Evaluating health information systems-related errors using the human, organization, process, technology-fit (HOPT-fit) framework. *Health Inform. J.* **2025**, *30*, 14604582241252763. [CrossRef] [PubMed]
23. Metin, B.; Özhan, F.G.; Wynn, M. Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics* **2024**, *13*, 4226. [CrossRef]
24. Hill, M. Airports Ill-Equipped to Deal with Major Cyber-Attacks. *InfoSecurity Magazine*. 2018. Available online: https://www.infosecurity-magazine.com/news/airports-illequipped-cyberattacks/#:~:text=increased%20technology%20usage%2C%20hyper%2Dconnectivity%2C%20data%2Dsharing%20obligations%2C%20customer,remote%20towers%20and%20airports%20as%20mega%20hubs (accessed on 12 November 2025).
25. Qatar Civil Aviation Authority. Aviation Cybersecurity Guidelines. 2019. Available online: http://books.caa.gov.qa/books/whlt/#p=1 (accessed on 27 May 2025).
26. Kör, B.; Metin, B. Understanding human aspects for an effective information security management implementation. *Int. J. Appl. Decis. Sci.* **2021**, *14*, 105–122. [CrossRef]
27. Pratt, M. What is GRC? The Rising Importance of Governance, Risk, and Compliance. *CIO*. 2023. Available online: https://www.cio.com/article/230326/what-is-grc-and-why-do-you-need-it.html (accessed on 9 July 2025).
28. Murphy, J.R.; Sukkarieh, M.; Haas, J.; Hriljac, P. *Airport Cooperative Research Program Report 140: Guidebook on Best Practices for Airport Cybersecurity*; FAA: Washington, DC, USA; Transportation Research Board: Washington, DC, USA; The National Academies Press: Washington, DC, USA, 2015.
29. Spaniel, D.; Eftekhari, P. *Hacking Our Nation's Airports: Cyber-Kinetic Threats to the Technologies Running Airport Operations*; Institute for Critical Infrastructure Technology: Washington, DC, USA, 2019.
30. Goudge, S. *Cyber Security and Resilience Symposium: Towards a Resilient Aviation Cyber Space*; ICAO MID: Amman, Jordan, 2019.

31. Lykou, G.A.; Anagnostopoulou, A.; Gritzalis, D. *Smart Airport*; PWC: New York, NY, USA, 2018.
32. Mutluturk, M.; Kor, B.; Metin, B. The Role of Edge/Fog Computing Security in IoT and Industry 4.0 Infrastructures: Edge/Fog-based Security in Internet of Things. In *Research Anthology on Edge Computing Protocols, Applications, and Integration*; IGI Global: Hershey, DC, USA, 2021. [CrossRef]
33. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access* **2020**, *8*, 207602–207618. [CrossRef]
34. ENISA. *Securing Smart Airports*; ENISA: Heraklion, Greece, 2016. Available online: https://www.enisa.europa.eu/publications/securing-smart-airports (accessed on 7 July 2025).
35. Mutluturk, M.; Metin, B. Mapping the Phishing Attacks Research Landscape: A Bibliometric Analysis and Taxonomy. *J. Theor. Appl. Inf. Technol.* **2023**, *101*, 21.
36. SITA. *2023 Air Transport IT Insights*; Société Internationale de Télécommunications Aéronautiques (SITA): Geneva, Switzerland, 2023.
37. IATA. *Air Transport Security: 2040 and Beyond*; International Air Transport Association: Montreal, QC, Canada, 2019.
38. Dursun, S.M.; Mutluturk, M.; Taskin, N.; Metin, B. An Overview of the IT Risk Management Methodologies for Securing Information Assets. In *Cases on Optimizing the Asset Management Process*; IGI Global: Hershey, PA, USA, 2022; pp. 30–47. [CrossRef]
39. Metin, B.; Duran, S.; Telli, E.; Mutlutürk, M.; Wynn, M. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation that Engenders a Security Culture. *Information* **2024**, *15*, 55. [CrossRef]
40. *ISO/IEC 27001:2022*; Information Technology—Security Techniques—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022.
41. Lufthansa Industry Solutions. Cyber Security Survey: Only One in Two Employees Believe Their Company is at Risk from Hackers. 2024. Available online: https://www.lufthansa-industry-solutions.com/de-en/newsroom-downloads/news/new-white-paper-and-survey-on-cyber-security (accessed on 9 November 2025).
42. Airports Council International (ACI). APEX in Cybersecurity Assessment Program. Available online: https://aci.aero/programs-and-services/apex/host-an-apex-review/apex-in-cybersecurity-assessment-program/ (accessed on 9 November 2025).
43. CER Directive. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, on the Resilience of Critical Entities. Official Journal of the European Union, L333/99. 2022. Available online: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng (accessed on 15 December 2025).
44. NIS2 Directive. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (OJ L 333, 27 December 2022, pp. 80–134). EUR-Lex. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed on 15 December 2025).
45. CRA. Cyber Resilience Act, 2024. European Parliament and the Council of the European Union. Available online: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html (accessed on 30 May 2025).
46. ICAO. Cybersecurity Culture in Civil Aviation. 2022. Available online: https://www.icao.int/sites/default/files/Security/documents/ICAO-Cybersecurity-Culture-in-Civil-Aviation_EN.pdf (accessed on 9 April 2025).
47. Turkish DGCA (Directorate General of Civil Aviation). Instruction on Cybersecurity for Civil Aviation Enterprises. 2022. Available online: https://web.shgm.gov.tr/documents/sivilhavacilik/files/mevzuat/sektorel/talimatlar/2022/SHT-Siber.pdf (accessed on 9 November 2025).
48. Filinovych, V.; Hu, Z. Aviation and the Cybersecurity Threats. *Adv. Econ. Bus. Manag. Res.* **2021**, *188*, 120–126.