Considerations regarding security risk management in modern air transport

Mihai NEACSU*,[1], Valentin SOARE[2], Gabriela-Liliana STROE[1,2]

*Corresponding author
[1]Faculty of Aerospace Engineering,
National University of Science and Technology POLITEHNICA Bucharest,
Splaiul Independentei 313, 060042, Bucharest, Romania
[2]INCAS – National Institute for Aerospace Research "Elie Carafoli",
B-dul Iuliu Maniu 220, Bucharest 061126, Romania,
micky969@ymail.com, soare.valentin@incas.ro, stroe.gabriela@incas.ro

DOI: 10.13111/2066-8201.2026.18.1.11

Received: 18 December 2025/ Accepted: 21 February 2026/ Published: March 2026

Abstract: *This paper presents an analysis of aviation security as a core priority of the aviation industry, alongside safety, and as an integral component of all operational activities. In the context of continuously evolving security threats, the effective management of aviation security has become increasingly critical. Airlines, airports, governments, international organizations, and other aviation stakeholders are actively engaged in enhancing and developing security capabilities. The paper emphasizes the importance of incident management, inter-organizational collaboration, and security assurance, which must remain uncompromised. Furthermore, it highlights the need for the aviation sector to continuously adapt to changing regulatory requirements and the challenges posed by the global security environment, particularly as operations expand and evolve. Strengthened security measures not only mitigate risks, but also contribute to improving operational efficiency, enhancing cooperation among aviation stakeholders, and incresing passenger confidence and satisfaction.*

Key Words: *security risk management, International Civil Aviation Organization (ICAO), risk assessment, Threat-Vulnerability-Consequence (TVC) model, air transport*

1. INTRODUCTION

Air transport plays a vital role in the global economy by enabling international connectivity, facilitating trade, tourism, and cultural exchange, and supporting economic development [8]. Due to its strategic importance and high visibility, the aviation sector has long been recognized as a potential target for acts of unlawful interference, making security a fundamental concern alongside safety. Consequently, aviation security is embedded in all operational activities and represents a core pillar of the aviation system [1].

In the contemporary security environment, aviation security extends beyond traditional physical protection measures and encompasses a complex system of policies, procedures, technologies, and coordinated actions aimed at preventing, detecting, and responding to security threats [10]. The evolving nature of threats to civil aviation has significantly increased the complexity of security management. While conventional threats such as hijacking and sabotage remain relevant, emerging risks include cyber-attacks, insider threats, the malicious use of unmanned aircraft systems (UAS), and the exploitation of digital and technological vulnerabilities [2, 3,

5]. These challenges are further amplified by the rapid growth of air traffic, increasing automation, and the global interconnection of aviation systems.

In response to this dynamic threat environment, security risk management has become a cornerstone of modern aviation security strategies. International organizations, particularly the International Civil Aviation Organization (ICAO), advocate a risk-based approach to aviation security that focuses on the systematic identification, assessment, and mitigation of threats and vulnerabilities [2]. This approach enables aviation stakeholders to prioritize risks, allocate resources efficiently, and implement proportionate security measures that balance effectiveness with operational efficiency and passenger facilitation. The gradual transition from prescriptive security requirements to performance-based and intelligence-driven frameworks reflects the need for adaptable and resilient security systems [8].

Security risk management in modern air transport is inherently a shared responsibility. It involves a wide range of stakeholders, including airlines, airport operators, air navigation service providers, regulatory authorities, law enforcement agencies, and international bodies [4]. Effective collaboration, information sharing, and coordination among these actors are essential to ensure a coherent and integrated aviation security system.

Moreover, incident management, continuous monitoring, and security assurance processes play a critical role in evaluating the effectiveness of implemented measures and supporting continuous improvement [1].

Beyond its primary role in threat mitigation, strengthened aviation security achieved through robust risk management practices also delivers broader organizational and systemic benefits. Effective security processes can reduce operational disruptions, enhance cooperation among aviation stakeholders, and improve passenger confidence and trust in air transport [10]. In an increasingly competitive, regulated, and security-sensitive environment, security risk management therefore represents not only a protective necessity but also a strategic asset for the aviation industry.

Against this background, this paper examines key considerations related to security risk management in modern air transport. It emphasizes the importance of a risk-based approach to aviation security, highlights current and emerging challenges, and underlines the role of regulatory compliance, collaboration, and continuous adaptation in addressing evolving security threats. The paper is therefore contributing to the ongoing discourse on enhancing the effectiveness, resilience, and sustainability of aviation security systems in a rapidly changing global security environment.

2. SECURITY RISK MANAGEMENT IN AIR TRANSPORT: CONCEPTUAL FRAMEWORK

In the aviation context, security risk is commonly understood as the combination of the likelihood of an intentional unlawful act and the severity of its potential consequences, taking into account existing vulnerabilities within the aviation system [1]. Unlike safety risks, which are generally associated with unintentional hazards and system failures, security risks arise from deliberate actions aimed at causing harm, disruption, or fear. These actions may target aircraft, passengers, crew, airport infrastructure, air navigation systems, or supporting information and communication technologies [10].

Security risk in air transport is typically analyzed through three interrelated components: threat, vulnerability, and consequence. A threat refers to the intent and capability of an adversary to carry out an unlawful act; vulnerability represents weaknesses that can be exploited; and consequence reflects the potential impact on human life, operations, infrastructure, and public

confidence [5]. Effective security risk management requires a comprehensive understanding of how these elements interact within a complex and interconnected aviation system.

The increasing digitalization and globalization of air transport have further expanded the scope of aviation security risks. Modern aviation systems rely heavily on automated processes, data exchange, and networked technologies, which introduce new vulnerabilities and attack vectors. As a result, security risk management must adopt a systemic and holistic perspective, recognizing aviation as a socio-technical system in which human, organizational, and technological factors are closely intertwined [7, 8].

Security risk management in aviation is based on a structured and continuous process aimed at identifying, assessing, mitigating, and monitoring security risks in a proactive and systematic manner [7]. In accordance with ICAO guidance, the aviation security risk management process is illustrated in Figure 1 [2].

Fig. 1 Security risk management in aviation [2]

A fundamental principle of modern aviation security is the adoption of a risk-based approach. Rather than applying uniform and prescriptive measures across all operations, risk-based security focuses on allocating resources and controls proportionally to the level of assessed risk. This approach allows aviation organizations to enhance security effectiveness while maintaining operational efficiency and passenger facilitation [8, 9]. It also supports adaptability, enabling security systems to respond more effectively to emerging threats and changing operational environments.

Security risk management in modern air transport is inherently collaborative and involves a wide range of stakeholders. Airlines, airport operators, air navigation service providers, security service providers, law enforcement agencies, intelligence services, and regulatory authorities all play distinct but interdependent roles in maintaining aviation security [5, 9].

Airports and airlines are responsible for implementing operational security measures and for identifying and reporting vulnerabilities within their activities. Regulatory authorities provide oversight, guidance, and enforcement, while law enforcement and intelligence agencies contribute threat information and response capabilities.
Effective coordination and information sharing among these stakeholders are essential to ensure a coherent and resilient security system [2].
Public-private partnerships and joint risk assessments have become increasingly important tools for enhancing security risk management. By fostering trust and collaboration, these mechanisms support timely decision-making and enable a more comprehensive understanding of the security risk landscape.

3. RISK ASSESSMENT METHODS IN AVIATION SECURITY

Risk assessment represents a central component of aviation security risk management, providing the analytical foundation for decision-making, prioritization, and resource allocation. In the context of modern air transport, risk assessment enables aviation stakeholders to systematically evaluate potential security threats, identify vulnerabilities, and estimate the potential consequences of unlawful acts [2].
By translating complex security environments into structured and comparable risk profiles, risk assessment supports the development of proportionate and effective security measures.
Unlike safety risk assessment, which often relies on historical data and probabilistic modelling, aviation security risk assessment must address intentional and adaptive adversaries. This characteristic introduces a higher degree of uncertainty and requires the integration of qualitative judgment, intelligence inputs, and scenario-based analysis [5]. Consequently, security risk assessment models must be flexible, iterative, and capable of incorporating both quantitative and qualitative information.

3.1 Threat-Vulnerability-Consequence (TVC) model

One of the most widely applied conceptual models in aviation security risk assessment is the Threat-Vulnerability-Consequence (TVC) framework.
This model defines risk as a function of three interdependent components: the likelihood of a threat, the level of vulnerability within the system, and the severity of potential consequences [6, 10].

- Threat assessment focuses on identifying adversaries, their intent, capabilities, and potential attack methods. This component is often informed by intelligence data and law enforcement analysis.
- Vulnerability assessment examines weaknesses in procedures, infrastructure, technology, and human performance that could be exploited by an attacker.
- Consequence assessment evaluates the potential impact of a successful attack, including loss of life, operational disruption, economic damage, and reputational effects.

The TVC model is particularly suited to aviation security due to its structured yet adaptable nature. It allows stakeholders to compare different threat scenarios and prioritize mitigation measures based on risk significance rather than prescriptive requirements [6, 8].
ICAO promotes variations of this model in its guidance material for aviation security risk assessment [1].

3.2 Qualitative and semi-quantitative risk assessment methods

Given the limited availability of reliable statistical data on security incidents and the adaptive behavior of adversaries, qualitative and semi-quantitative methods are commonly used in aviation security risk assessment. Qualitative approaches rely on expert judgment, structured interviews, workshops, and scenario analysis to evaluate threats and vulnerabilities using descriptive scales (e.g. low, medium, high) [10].

Semi-quantitative methods build on qualitative assessments by assigning numerical values or scores to risk factors. Risk matrices are a typical example, combining likelihood and consequence scores to derive an overall risk level.

These tools support transparency and consistency in decision-making while remaining flexible enough to accommodate uncertainty [5].

While these methods do not provide precise probability estimates, they are particularly valuable in security contexts where uncertainty is high and intelligence information may be sensitive or incomplete. Their effectiveness depends heavily on the expertise of participants and the quality of the assessment process.

3.3 Scenario-based risk assessment

Scenario-based risk assessment is a widely used approach in aviation security, especially for evaluating low-probability, high-consequence events. This method involves the systematic development and analysis of plausible attack scenarios, taking into account attacker behavior, system responses, and cascading effects [8].

In aviation security, scenarios may include attacks on aircraft, airport terminals, air cargo operations, or cyber systems. Each scenario is assessed in terms of threat credibility, system vulnerabilities, and potential consequences. Scenario-based assessments are particularly useful for testing the robustness of existing security measures and for identifying gaps in preparedness and response capabilities [2]. This approach also supports training, exercises, and contingency planning by enabling stakeholders to visualize complex threat situations and evaluate their ability to respond effectively. Effective risk assessment models must be embedded within broader aviation security management and governance frameworks. Risk assessment should not be treated as a one-time exercise but as a continuous and iterative process that supports strategic planning, operational decision-making, and performance monitoring [2]. Key elements of successful integration include:

- Regular review and updating of risk assessments;
- Use of assessment results to prioritize mitigation measures;
- Documentation and traceability of decisions;
- Feedback mechanisms and security assurance activities.

By integrating risk assessment into daily operations and management processes, aviation organizations can enhance their ability to anticipate emerging threats, respond proactively, and continuously improve security performance.

4. APPLICATION OF THE THREAT-VULNERABILITY-CONSEQUENCE (TVC) MODEL FOR AN AIRPORT OPERATOR

This chapter applies the Threat-Vulnerability-Consequence (TVC) model to illustrate how an airport operator can conduct a structured security risk assessment within the framework of modern aviation security risk management. The objective is to identify credible threat scenarios, assess relevant procedural and physical vulnerabilities, and estimate potential operational and

societal consequences. The analysis is conceptual and illustrative in nature and reflects internationally accepted practices promoted by ICAO and other aviation security bodies [1, 2]. The TVC model defines risk as the interaction between the likelihood of a threat, the existence of exploitable vulnerabilities, and the magnitude of potential consequences. This structured approach enables airport operators to prioritize risks, support decision-making, and implement proportionate mitigation measures aligned with a risk-based security philosophy [8].

Threat identification represents the first step in the TVC assessment process. For an airport operator, credible threat scenarios are typically derived from intelligence information, historical incident analysis, and assessments of the airport's operational profile and environment [10]. Common credible threat scenarios for a medium-to-large international airport may include:

- Insider threats involving authorized personnel exploiting access privileges;
- Unauthorized access to airside or restricted security areas;
- Use of improvised weapons or prohibited items in terminal public areas;
- Cyber-enabled attacks targeting airport operational systems;
- Disruption of airport operations through coordinated acts of unlawful interference.

These threats are considered credible due to their feasibility, historical precedent, and potential attractiveness to adversaries. Threat assessment focuses not only on intent but also on the capability of potential attackers and the attractiveness of the airport as a target within the broader aviation system [5]. Once credible threats are identified, the assessment of vulnerabilities focuses on weaknesses that could be exploited to enable or facilitate an unlawful act. For an airport operator, vulnerabilities may arise from procedural, physical, technological, or human factors [1]. Procedural vulnerabilities may include:

- Inconsistent application of access control procedures;
- Insufficient oversight of third-party contractors;
- Gaps in training or awareness among airport personnel;
- Limited coordination between airport security and external agencies.

Physical vulnerabilities may relate to:

- Design characteristics of terminal public areas;
- Perimeter fencing and surveillance limitations;
- Shared-use or high-density operational spaces;
- Aging infrastructure not originally designed for current threat profiles.

The vulnerability assessment evaluates the effectiveness of existing controls and identifies areas where safeguards may be insufficient, outdated, or inconsistently applied. This process emphasizes that vulnerabilities do not imply failure but rather highlight opportunities for targeted improvement [8]. The consequence component of the TVC model examines the potential impacts of a successful security breach. For airport operators, consequences extend beyond immediate physical damage and may affect operational continuity, public confidence, and broader societal interests [10]. Operational consequences may include:

- Temporary or prolonged closure of terminals or runways;
- Disruption to passenger flows and airline schedules;
- Financial losses due to delays, cancellations, and recovery measures;
- Increased regulatory scrutiny and resource demands.

Societal consequences may involve:

- Loss of life or injury;
- Psychological impact on passengers and staff;
- Erosion of public trust in aviation security;

- Reputational damage to the airport and national aviation system.

The assessment of consequences considers both direct and indirect effects, recognizing that even low-probability events may warrant attention if potential impacts are severe. This aligns with the precautionary principles underpinning aviation security management [2].

By integrating threat likelihood, vulnerability exposure, and consequence severity, the airport operator can evaluate overall risk levels for each scenario. Risks associated with high-impact consequences and exploitable vulnerabilities are prioritized for mitigation, even where threat likelihood is uncertain [5].

Risk evaluation supports decision-making by enabling airport management to:

- Prioritize security investments;
- Adjust operational procedures;
- Enhance coordination with stakeholders;
- Implement layered and proportionate security measures.

This structured prioritization ensures that security enhancements are targeted and evidence-based rather than reactive or purely compliance-driven.

Table 1 – Threat-Vulnerability-Consequence (TVC) risk matrix for an airport operator

Threat Scenario	Key Vulnerabilities	Operational Consequences	Societal Consequences	T	V	C	Overall Risk Score (T×V×C)	Risk Level
Insider threat involving authorized personnel	Inadequate background checks; limited access monitoring; insufficient security culture	Disruption of operations; closure of restricted areas; regulatory non-compliance	Loss of public trust; reputational damage; potential casualties	3	4	5	60	High
Unauthorized access to airside or restricted areas	Gaps in access control; perimeter surveillance limitations; shared operational spaces	Flight delays/ cancellations; aircraft ground damage	Passenger anxiety; confidence erosion	3	3	4	36	Medium-High
Attack in terminal public areas	Open terminal design; high passenger density; limited pre-screening	Terminal evacuation; disruption of passenger processing; revenue loss	Injuries/ fatalities; psychological impact	2	4	5	40	High
Cyber-attack on airport operational systems	Dependence on digital systems; limited IT-physical security integration	Degradation of airport systems; delays in check-in, baggage, airside coordination	Public confidence loss; indirect safety concerns	3	3	3	27	Medium
Disruption from coordinated unlawful interference	Fragmented stakeholder coordination; delayed information sharing	Prolonged operational disruption; emergency response escalation	National-level reputational impact; public perception of vulnerability	2	4	5	40	High

The risk rating is assessed on a 1-5 scale based on three dimensions: Threat Likelihood (T), Vulnerability Exposure (V), and Consequence Severity (C), where 1 represents very low and 5 represents very high levels for each factor, as follows:
Threat Likelihood (T): 1 = Very Low, 2 = Low, 3 = Medium, 4 = High, 5 = Very High
Vulnerability Exposure (V): 1 = Very Low, 2 = Low, 3 = Medium, 4 = High, 5 = Very High
Consequence Severity (C): 1 = Very Low, 2 = Low, 3 = Medium, 4 = High, 5 = Very High
The overall risk score is calculated as the product of Threat Likelihood (T), Vulnerability Exposure (V), and Consequence Severity (C).

$$\text{Overall Risk Score} = T \times V \times C \quad (1)$$

The risk matrix presented in table 1 is illustrative and non-sensitive, using qualitative scales commonly referenced in aviation security literature [2, 8].
The numerical scoring allows a semi-quantitative assessment of risk by combining likelihood, vulnerability, and consequence into a single risk score, which enhances comparability across scenarios.
Risk levels are categorized as:

- Low (green): 1-15;
- Medium (yellow): 16-30;
- Medium-High (orange): 31-45;
- High (red): 46-60.

The matrix illustrates how the interaction between threat credibility, exploitable vulnerabilities, and consequence severity determines overall risk levels. Threats associated with high-impact societal consequences, such as insider threats or attacks in terminal public areas, are prioritized even when likelihood is uncertain. This approach reflects the precautionary and risk-based philosophy promoted by ICAO [2].
The qualitative risk levels (Medium, Medium-High, High) support decision-making and prioritization, rather than precise prediction. For airport operators, such a matrix enables:

- Targeted allocation of security resources;
- Identification of areas requiring procedural reinforcement or infrastructure investment;
- Enhanced coordination with law enforcement and regulatory authorities;
- Continuous review as threat environments and operational contexts evolve [5, 10].

The application of the TVC model demonstrates the value of structured risk assessment as a practical management tool for airport operators. By systematically linking threats, vulnerabilities, and consequences, the model supports transparency, accountability, and continuous improvement in security decision-making [8]. Furthermore, the TVC approach reinforces the importance of collaboration, information sharing, and regular review. As threat environments and operational contexts evolve, risk assessments must be updated to maintain their relevance and effectiveness. In this sense, the TVC model contributes not only to risk mitigation but also to the resilience and sustainability of airport operations.

5. CONCLUSIONS

This paper has examined the theoretical and practical aspects of security risk management in modern air transport, with a particular focus on the application of structured risk assessment models. The analysis demonstrates that aviation security is a multidimensional and dynamic domain, requiring the integration of threat intelligence, operational procedures, infrastructure safeguards, and stakeholder collaboration.

A central finding is the critical value of a risk-based approach, exemplified through the Threat-Vulnerability-Consequence (TVC) model. The TVC framework provides airport operators and aviation stakeholders with a structured methodology to identify credible threats, assess vulnerabilities, and estimate the potential operational and societal impacts of security incidents. By integrating qualitative judgments, scenario-based assessments, and semi-quantitative scoring, risk models enable informed decision-making and prioritization of mitigation measures. The illustrative TVC risk matrix presented in this paper underscores how such tools support transparency, consistency, and accountability in airport security management.

The study also highlights the essential role of international, regional, and national regulatory frameworks in shaping aviation security practices. Compliance with ICAO Annex 17 standards, EU regulations, and national security programs ensures that risk assessments are aligned with globally recognized requirements, while also enabling adaptability to evolving threats. Effective implementation requires not only adherence to prescriptive rules but also proactive collaboration among airlines, airport operators, regulators, law enforcement, and intelligence agencies.

Emerging threats, including cyber-attacks, insider risks, and coordinated unlawful interference, underscore the need for continuous monitoring and adaptability. Security risk management cannot be static, it must evolve in response to changes in technology, operational environments, and adversary tactics. Scenario-based and hybrid assessment methods provide practical tools for anticipating such risks and testing the robustness of mitigation measures.

From an operational perspective, strengthened security has broader organizational and systemic benefits. Effective risk management enhances operational efficiency, improves coordination among stakeholders, and strengthens passenger confidence and public trust. It also serves as a strategic asset, allowing airports and airlines to maintain resilience while complying with increasingly complex regulatory requirements.

In conclusion, modern air transport security requires a holistic, risk-informed, and collaborative approach. The integration of structured risk assessment models, regulatory compliance, and continuous improvement processes is essential for safeguarding the aviation system against evolving threats.

Future research and practice should focus on refining quantitative and hybrid risk assessment methods, incorporating emerging technologies, and fostering enhanced information sharing and stakeholder collaboration. By doing so, the aviation industry can continue to ensure both safety and security while supporting the efficiency, resilience, and sustainability of global air transport operations.

REFERENCES

[1] * * * International Civil Aviation Organization (ICAO). *Annex 17 – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Twelfth Edition, July 2022.

[2] * * * International Civil Aviation Organization (ICAO), *Global Aviation Security Plan (GASeP)*, ICAO, 2017.

[3] * * * International Civil Aviation Organization (ICAO). *Global Cyber Risk Considerations* (Doc 10213 – Restricted), First edition (advance unedited), 2025.

[4] * * * European Commission. *Regulation (EC) No 300/2008 on common rules in the field of civil aviation security.*

[5] A. R. Thomas, *Aviation Security Management. The Context of Aviation Security Management,* Volume **1**, **2**, and **3**, Praeger Security International, 2008.

[6] C. Cioacă, *Master - Extreme risk management tool in aviation security systems*, 2014.

[7] E. Dudek, K. Krzykowska-Piotrowska, M. Siergiejczyk, Risk management in (air) transport with exemplary risk analysis based on the tolerability matrix, *Transport Problems, Silesian University of Technology*, Faculty of Transport, vol. **15** (2), 2020.

[8] J. C. Price and J. S. Forrest, *Practical Aviation Security: Predicting and Preventing Future Threats*, Butterworth-Heinemann, 2016.
[9] J. Kolesár and M. Petruf, Risk management in the sphere of civil airport protection againts of unlawfull interference, *Annals of Faculty Engineering Hunedoara - International Journal of Engineering*, 2012.
[10] K. M. Sweet, *Aviation and Airport Security: Terrorism and Safety Concerns,* Second Edition, CRC Press, 2008.