IATA Annual Security Report

2025 Edition

Support by Our Strategic Partners

Albans Management SA
Alpha Airport MXP S.p.A.
ASM Security Management Company Limited
Aviation Co-ordination Services (Pty) Ltd
Beijing Zhongdun Anmin Analysis Technology Co., Ltd
CEIA S.p.A.
Dragonfly from Dow Jones
Ground Controls
Gozen Security Services Inc.
LCB Worldwide
MedAire
Nuctech Company Limited
Osprey Flight Solutions
Securiport
SITA

DISCLAIMER

The content, data, and information (the "Content") contained in this publication ("Publication"), is provided for information purposes only and is made available to you on an "AS IS" and "AS AVAILABLE" basis.

IATA has used reasonable efforts to ensure the Content of this Publication is accurate and reliable. We, however, do not warrant, validate, or express any opinions whatsoever as to the accuracy, genuineness, origin, tracing, suitability, availability or reliability of the sources, completeness, or timeliness of such Content. IATA makes no representations, warranties, or other assurances, express or implied, about the accuracy, sufficiency, relevance, and validity of the Content. IATA's observations are made on a best efforts and non-binding basis, and shall not be deemed to replace, interpret, or amend, in whole or in part, your own assessment and evaluation or independent expert advice. Nothing contained in this Publication constitutes a recommendation, endorsement, opinion, or preference by IATA.

IATA has no obligation or responsibility for updating information previously furnished or for assuring that the most up-to-date Content is furnished. IATA reserves the right to remove, add or change any Content at any time. Links to third-party websites or information directories are offered as a courtesy. IATA expresses no opinion on the content of the websites of third parties and does not accept any responsibility for third-party information. Opinions expressed in advertisements appearing in this publication are the advertiser's opinions and do not necessarily reflect those of IATA. The mention of specific companies or products in advertisements does not imply that they are endorsed or recommended by IATA in preference to others of a similar nature which are not mentioned or advertised.

This Publication is not intended to serve as the sole and exclusive basis for assessment and decision making and is only one of many means of information gathering at your disposal. You are informed to make your own determination and make your own inquiries as you may deem necessary and suitable. You shall independently and without solely relying on the information reported in this Publication, perform your own analysis and evaluation regarding the nature and level of information you may require, based upon such information, analyses, and expert advice as you may deem appropriate and sufficient, and make your own determination and decisions pertaining to the subject matter under consideration.

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, IATA DISCLAIMS ANY REPRESENTATION OR WARRANTY (I) AS TO THE CONDITION, QUALITY, PERFORMANCE, SECURITY, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THIS PUBLICATION AND CONTENT; OR (II) THAT THE ACCESS TO OR USE OF THIS PUBLICATION (INCLUDING ANY AUTOMATED FEEDS OR OTHER DELIVERY MODES) OR ANY CONTENT SUPPLIED OR CONTRIBUTED TO THIS PUBLICATION BY THIRD PARTIES, WILL BE UNINTERRUPTED, ACCURATE, THE MOST UP TO DATE, COMPLETE OR ERROR-FREE. IATA EXCLUDES ALL LIABILITY (TO THE EXTENT PERMITTED BY APPLICABLE LAW) FOR ANY COSTS, LOSSES, CLAIMS, DAMAGES, EXPENSES OR PROCEEDINGS OF WHATEVER NATURE INCURRED OR SUFFERED BY YOU OR ANY OTHER PARTY ARISING DIRECTLY OR INDIRECTLY IN CONNECTION WITH THE USE OF THIS PUBLICATION OR ANY CONTENT CONTAINED OR ACCESSED THEREFROM, OR DUE TO ANY UNAVAILABILITY OF THIS PUBLICATION IN WHOLE OR IN PART.

Contents

1 How to Use This Report

- **Gain a clear, strategic understanding** of the aviation security, geopolitical, and regulatory developments that shaped global civil aviation in 2025. Thus, enabling more informed risk-based decision-making across your organisation.

- **Make confident operational and cross-border decisions** by understanding how evolving threats, conflict-zone dynamics, and State regulatory actions may affect airspace availability, upstream/downstream compliance obligations, and network resilience.

- **Identify emerging risks and opportunities** affecting customers, workforce, assets, and supply chain, including conflict-zone exposure, GNSS interference trends, surveillance mandates, and changes in international security frameworks.

- **Learn the actions and adaptations** airlines, regulators, and airports can take now to strengthen operational resilience, enhance SeMS performance, and prepare for the next phase of global security and geopolitical risk management.

2 Executive Summary

2025 was perhaps the most geopolitically volatile year for civil aviation since MH17 in 2014, with multiple conflicts and security events directly affecting airspace availability, operational continuity, and regulatory policy. Spillover from the Iran–Israel conflict reached Doha, Chinese naval live-fire exercises disrupted trans-Tasman routes, drone strikes closed airports in Sudan, and border tensions in South and Southeast Asia triggered sudden airspace shutdowns. These events were compounded by persistent GNSS interference and an expanding spectrum of grey-zone threats and projection of power activities.

Throughout the year, IATA's strategic direction in aviation security was guided by its member airlines through the Security Advisory Council (SAC) and the Geopolitical Risk Task Force (GRTF), which continued to provide structured, operationally grounded advice reflecting member strategic interests. Their guidance shaped IATA's advocacy priorities across airspace security, conflict-zone risk management, GNSS resilience, and performance-based oversight, ensuring that industry positions remain aligned with real world operational risk and airline decision making needs.

Despite this environment, the aviation industry, led by airline operational and security teams, demonstrated exceptional resilience and maturity in managing conflict-zone risk. Operators applied ICAO Doc 10084 principles with increasing discipline, including continuous monitoring, intent-capability assessment, and rapid routing decisions based on multi-source intelligence.

Regulatory divergence widened across several domains, notably hold baggage reconciliation, surveillance mandates, GNSS interference reporting, and non-harmonized NOTAM practices. Industry priorities increasingly converged on airspace security, GNSS resilience, performance-based oversight, and One-Stop Security and Recognition of Equivalence frameworks. IATA advocacy focused on modernizing legacy requirements, promoting proportional and risk-based regulation, and strengthening civil–military coordination to prevent both deliberate and accidental harm to civil aviation.

Air cargo security remained under pressure from geopolitical fragmentation and the evolving incendiary device threat, yet the sector again demonstrated adaptability and growth. Parallel progress was achieved in Security Management Systems (SeMS), digital trust initiatives, and the Aviation Security Trust Framework, supporting a shift toward data-driven assurance and smarter oversight.

Looking ahead, 2026 marks a transition from framework development to operational implementation. Key initiatives in airspace risk management, GNSS mitigation, digital trust, and real-time coordination will move into daily practice across airlines, regulators, and ANSPs. Sustaining high levels of safety and security in an increasingly unstable global environment will depend on stronger military–civil coordination, improved navigation resilience, and globally harmonized information-sharing mechanisms.

3 Regulatory and International Engagement

ICAO AVSEC Panel

- Endorsement of new Hold Baggage Screening, Handling & Processing guidance (including a dedicated section on "Hold Baggage Reconciliation - the accompanied vs. unaccompanied process").
- New proposal for Amendment 19 to Annex 17 with the expansion of the One-Stop Security concept to aircraft security checks and searches (Standard 4.3.1). ICAO Council accepted in November 2025 to share the amendment for gathering State's comments (State Letter issued on 12 December 2025). Final proposals will be presented to the Council for adoption in June 2026. Applicability date is expected for November 2026.
- During the review of AVSECP/36 report, the ICAO Aviation Security Committee supported AVSEC Panel to continue to consider One-Stop Security concept in Annex 17 more broadly in the near future.

ICAO General Assembly

- Strong Member State debate on GNSS interference, including calls for ICAO to establish a global reporting framework.
- Increased pressure to address unannounced military exercises after the Tasman Sea, Sudan, and Gulf incidents.
- Assembly encourages all Member States, including those involved in ICAO security bodies, to utilize industry technical input to further enhance safety and security (paragraph 13.47 of the report on the Security Agenda item, A42-WP/645 following IATA's A42-WP/241).

EU Regulatory Evolution (SAGAS, EASA, EC)

- EASA launch of formal review into airspace conflict-zone information harmonization.
- EC–TSA engagement on oversight interoperability and privacy standards, triggered by several EU airline concerns.

United States (TSA, FAA)

- TSA's 2025 letter strengthens its position on security information reporting and operator responsibilities.
- In 2025, IATA engaged the U.S. Transportation Security Administration (TSA) under Executive Order 14219 on regulatory review and efficiency, advocating for modernization of aviation security regulation while maintaining robust security outcomes. IATA urged the TSA to reduce duplication by recognizing equivalence between international standards and U.S. requirements, particularly through acceptance of foreign carriers' Aircraft Operator Security Programmes (AOSPs) supplemented only by targeted local requirements where gaps exist. This approach was presented to streamline compliance while preserving security effectiveness.
- IATA also called for reform of outdated operational requirements, notably the Positive Passenger/Bag Match (PPBM) mandate, highlighting that advances in explosive detection systems and universal hold baggage screening under ICAO standards render physical reconciliation unnecessary and operationally disruptive. Airlines were advised that continued reliance on PPBM contributes to delays, weight-and-balance risks, and limited security benefit compared to modern screening regimes.

- More broadly, IATA promoted a shift toward performance-based security using Security Management Systems (SeMS), supported by digital trust frameworks and verifiable credentials, enabling continuous self-assessment and targeted regulatory oversight. This model was positioned as essential for addressing emerging threats such as cyber and foreign interference while reducing administrative burden and enabling risk-based, data-driven supervision. IATA invited the TSA to work collaboratively with industry to implement these reforms and align U.S. practices with evolving international standards

- FAA–IATA engagement on military–civil NOTAM reform, following near real-time deficiencies demonstrated in 2025.

Other Matters

In 2024–2025, IATA led industry advocacy in response to the German civil aviation authority's decision to levy security inspection fees directly on airlines for aviation security oversight activities at German airports. IATA challenged this policy as inconsistent with ICAO principles requiring that charges be cost-related, transparent, proportionate, and non-discriminatory, and raised concerns regarding conflicts of interest, the absence of risk-based prioritization, and limited consultation with international partners.

IATA advised member airlines that, while opposing the measure in principle, any legal challenge must be made individually for each invoice and within the applicable statutory deadline. Airlines were encouraged to coordinate closely with their legal and security functions when determining whether to contest charges. IATA further advocated that mature Security Management Systems (SeMS) should be recognized as a basis for proportionate oversight and that inspection regimes should support security outcomes rather than revenue generation. The issue was escalated through formal correspondence with German authorities and through ICAO advocacy to reinforce global principles on the funding of national aviation security oversight.

4 One Stop Security (OSS) and Recognition of Equivalence (RoE)

2025 marked a turning point with ICAO's new Hold Baggage Reconciliation guidance, enabling "OSS for Hold Bags" as a practical early option.

Growing concerns from upstream States about downstream extraterritorial demands (e.g., requiring additional searches of aircraft or CCTV access).

Explicit link between OSS, RoE Collaborative Arrangements, and global hub competitiveness, increasingly highlighted by Member States.

- IATA and its member airlines fully support States and airport operators in conceptualizing, designing, and implementing One-Stop Security (OSS) and Recognition of Equivalence (RoE) collaborative arrangements, recognizing their potential to enhance security outcomes while improving passenger flow, operational efficiency, and hub competitiveness.
- Recognition of Equivalence (RoE) allows for the mutual recognition of equivalent robust security measures applied at that point of origin, that in turn facilitates the elimination of potential redundant measures and security controls and opens the way for OSS initiatives.
- Global implementation remains limited, especially outside Europe, with fewer than a dozen non-European States applying OSS through unilateral, bilateral, or multilateral arrangements.
- Major implementation challenges persist, including the lack of an Industry and ICAO-endorsed economic modelling framework, combined with infrastructure and master-planning constraints, regulatory fragmentation, and extraterritorial demands imposed by *downstream States* that do not fully accept the controls applied by *upstream States*.
- A practical early focus for States and airports not yet convinced about full economic and operational benefits of OSS is the deployment of hold-baggage OSS initiatives, where updated ICAO guidance and existing technical criteria provide a lower-complexity, operationally credible pathway before expanding to full passenger-flow OSS.

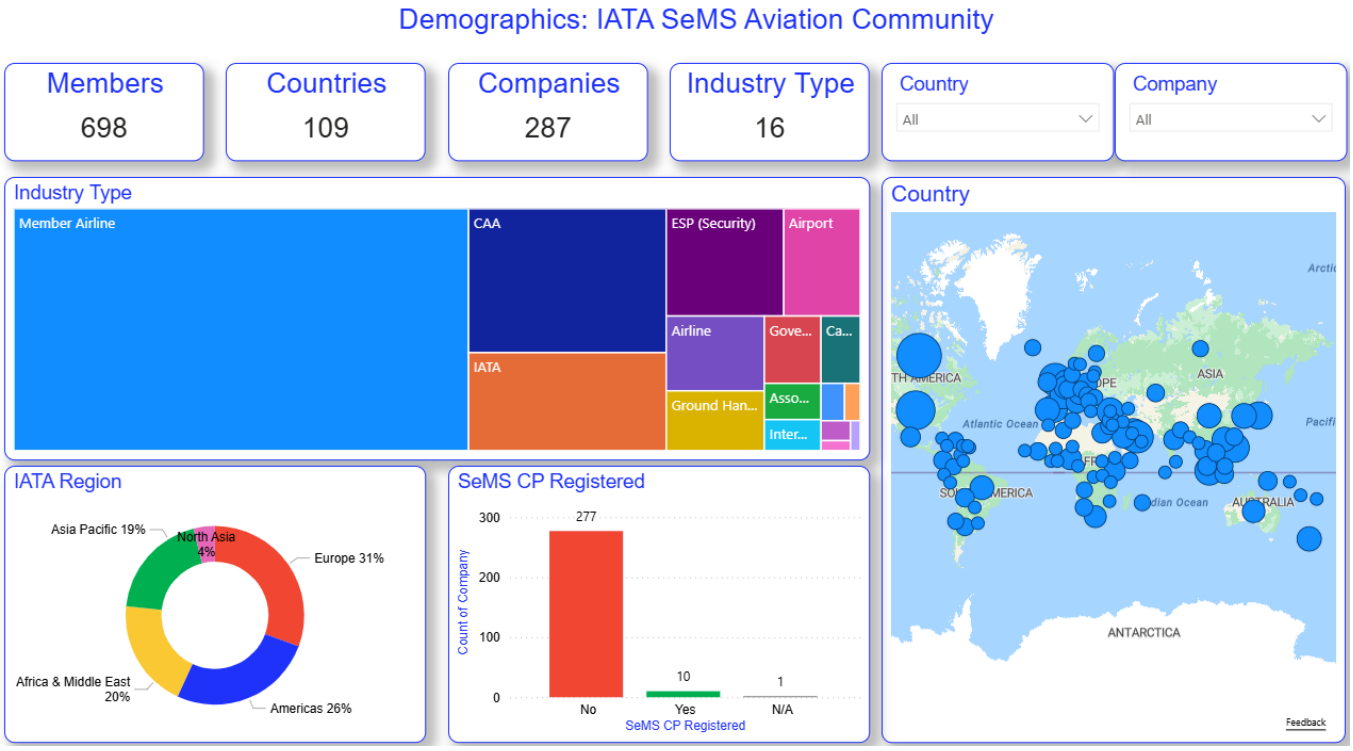
5 Security Management System (SeMS)

In 2025, IATA continued to strengthen global adoption of Security Management Systems (SeMS) and advance the industry's transition toward performance-based security oversight. The first wave of SeMS Certification pilots produced measurable operational insights and helped regulators better understand how data-driven assurance and predictive methodologies can reduce compliance gaps and inspection workload. The release of the *SeMS Manual – 9th Edition* introduced a new predictive anchor-question methodology, reinforcing the shift toward intelligence-led risk identification and continuous monitoring.

Throughout the year, IATA promoted stronger alignment between **Annex 17** (Security) and **Annex 19** (Safety Management), particularly in risk assessment, assurance models, and performance indicators. This effort was supported by the publication of the new **IATA SeMS Strategy** in May 2025 and a series of global engagements, including a liaison visit to Bergamo, a capacity-building workshop in Beijing, and the **Aviation Security Forum in November 2025**, which convened over 100 participants to explore next-generation SeMS adoption. In parallel, IATA has commissioned the UK CAA International to conduct a regulatory study examining how SeMS Certification could integrate into existing oversight structures and what adjustments are required to support true performance-based oversight.

Since December 2022, IATA has been hosting an international SeMS Aviation Community, open to all industry stakeholders willing to exchange SeMS-related information and reference documents. After three full years, this holistic community brings together nearly 700 members from more than 100 countries, representing almost 300 organizations across 16 different stakeholder profiles.

Stakeholders and aviation colleagues interested in joining the SeMS Aviation Community are invited to contact aviationsecurity@iata.org.



[Source IATA - 27 January 2026]

5.1 Looking Ahead to 2026

In 2026, IATA will accelerate development of the digital-trust architecture underpinning SeMS and the Aviation Security Trust Framework (ASTF). This includes building an AI-powered self-assessment tool, validated against historical compliance data, capable of projecting risk trends and supporting smart-sampling oversight techniques. Verifiable Credential (VC) functionality will be incorporated to enable operators and supply-chain partners to securely "hash" evidence such as training records, audit outputs, process documentation. This will allow regulators to verify compliance remotely, instantly and without duplication.

Work will continue multilingual capability (Mandarin language as priority), strengthening adoption pathways across Asia and other key markets.

Stakeholder engagement efforts will expand through regulator workshops, operator training, and SAC-led advocacy under the narrative **"digital trust = smarter oversight."** These initiatives aim to build familiarity with VC-enabled assurance and prepare States for integrating ASTF-validated evidence into their oversight cycles.

Regulatory alignment will focus on supporting ICAO's movement toward performance-based oversight, advocating for acceptance of VC-backed evidence, and positioning ASTF as the global framework for trusted security attestations. To ensure long-term sustainability, IATA will explore hosting services within IATA Connect, supported by optional premium trust services and aggregated insights to guide capacity-building and policy development.

6 Air Cargo Security

2025 Air Cargo Security Overview

2025 proved to be another challenging year for the air cargo sector, with multiple compounding factors affecting security and cargo flows. These included fragmented aviation security policies, tariffs and other protectionist measures, geopolitical conflict and resulting airspace closures, as well as the ongoing threat posed by Improvised Incendiary and Explosive Devices.

Despite these challenges, the air cargo sector once again demonstrated remarkable resilience and an ability to adapt quickly to an evolving threat landscape. In 2025, the industry recorded at least eight consecutive months of air cargo volume growth. Looking ahead to 2026, IATA forecasts air cargo volumes to increase by approximately 2.6%, with total volumes expected to reach 71.6 million tons.

Nevertheless, significant security challenges remain. To sustain the sector's positive trajectory and long-term security health, effective industry–government partnerships, respect for the international aviation security framework, and a continued commitment to innovation and enhancement of air cargo security are essential.

IATA Cargo Security Working Group (CSWG)

The IATA Cargo Security Working Group (CSWG), established as a subgroup of the Cargo Management Board (CMB), is responsible for reviewing and addressing all matters related to cargo security. The CSWG is composed of 15 airline members, together with observer participants.

In 2025, the CSWG had a particularly active year, holding its four scheduled quarterly meetings in addition to a series of extra meetings and workshops focused on leading IATA's Consignment Security Declaration (CSD) and e-CSD reform. Besides constant advocacy on AVSEC legislative reforms, CSWG's priorities for 2025 also included:

- Leading and progressing IATA's CSD/e-CSD reform
- Ongoing response to the 2024 incendiary incidents impacting air cargo
- Outreach to and engagement with AVSEC Regulators
- Monitoring of AVSEC technology and innovation
- Routine review of cargo security content in IATA's manuals, polices, standards and training packages

IATA Improvised Incendiary Device (IID) Guidance – Version 2

Following release of IATA IID Guidance in February 2025, CSWG initiated a revision in May. The enhanced Version 2 was released in September 2025 and introduces the following key updates and additions:

- Expanded material on incendiaries, incendiary weapons and incendiary devices
- Three newly recommended security measures (to mitigate against IID risks)
- A case study on information sharing

Version 2 is available via the IATA – Cargo Security website.

Air Mail Security

Following the incendiary incidents targeting air cargo, mail and supply chains in 2024–2025, air mail security became a key priority. Throughout 2025, IATA worked closely with partners at ICAO and the UPU to assess evolving security challenges and identify opportunities to strengthen the security and resilience of the global air mail system.

CSD/e-CSD Reform Initiative

In 2025, IATA advanced the CSD and e-CSD Reform Initiative, led by the CSWG and an extended Reform Group including approximately 60 supply chain stakeholders, such as airlines and freight forwarders, and IT service providers. The initiative seeks to modernize the CSD and e-CSD processes to improve usability, adoption, and implementation across the industry.

Two in person workshops and a series of meetings were held throughout 2025, identifying key challenges and priorities to be incorporated into the reform programme. Building on this strong engagement, the initiative has now entered the solution phase, with a draft reform package scheduled for broad consultation with industry and government stakeholders in early 2026

Policy Review

Following the IID incidents in July 2024 and early 2025, and in response to the broader evolving threat environment, several States and regions undertook legislative reviews and amendments to their national air cargo security policies. Throughout 2025, IATA participated in multiple review and consultation processes, supporting its members through a coordinated, unified, and objective industry position. IATA's advocacy and direct engagement resulted in several successful interventions, leading to revisions of initial policy proposals to better align with industry operational realities and risk-based, proportionate air cargo security practices.

Multilateral Engagement

Through its membership of various international Working Groups and Committees, IATA participated in multilateral meetings, events and discussions covering air cargo security matters throughout 2025. This included the International Civil Aviation Organization (ICAO) Aviation Security Panel (AVSECP) and Working Group on Air Cargo Security (WGACS), ICAO Dangerous Goods Panel, the World Customs Organization (WCO) SAFE Working Group and Private Sector Consultative Group, joint Committees with the Universal Postal Union UPU, and various regional trade association meetings and engagement with other UN System organizations.

7 Workshops, Conferences, & Forums

7.1 Civil Aviation Security in Africa, the Middle East and Asia (CASE II) ECAC & the Kingdom of Saudi Arabia – February 2025

In 2025, IATA played a central leadership role in advancing risk-based passenger security and accelerating global understanding and adoption of One-Stop Security (OSS). Through sustained advocacy and technical engagement with States, regulators, and airports, IATA strengthened alignment on Recognition of Equivalence (RoE), Hold Baggage Security (HBS) reform, and the progressive removal of unnecessary re-screening at transfer points. A major milestone was IATA's contribution to the **Interregional Seminar on Privatization of Aviation Security & One Stop Security** held in Riyadh from 24–26 February 2025, where I led key sessions outlining operational benefits, regulatory considerations, and practical implementation pathways needed for wider OSS adoption.

These engagements reinforced OSS as a scalable, Annex-17-compliant framework that improves facilitation, reduces duplication, enhances hub competitiveness, and supports intelligence-led aviation security. IATA's leadership helped shape regional and international regulatory thinking throughout 2025 and established strong foundations for broader OSS implementation in 2026 and beyond.

7.2 Leaders Week (Sydney, Australia) – March 2025

The 2025 Sydney Leaders Aviation Security Week brought together senior government, airline, and regulatory security leaders from across the global aviation ecosystem for a focused, high-level exchange on current and emerging security challenges. Hosted at Qantas Headquarters on 19 March, the event convened more than 50 participants spanning international carriers, national authorities, security intelligence agencies, and industry bodies. The closed-door, in-person setting enabled strategic discussions on policy alignment, operational risks, and leadership approaches in an increasingly complex and dynamic threat environment.

Keynote and opening remarks from senior officials—including Australia's Department of Home Affairs, Transport Canada, the UK Department for Transport, and the Civil Aviation Authority of New Zealand—set the global context for evolving cyber, infrastructure, and physical security risks. Subsequent plenary discussions highlighted the increasing importance of visionary and diverse leadership in shaping aviation security strategy, with emphasis on inclusivity, collaboration, and a strong pipeline of future security professionals.

A major theme throughout the program was the integration of security, safety, and facilitation imperatives. Panels examined emerging threat vectors and the need for intelligence-driven, risk-based responses that maintain operational continuity and customer experience. The Security Threat Context session underscored the interconnected nature of cyber, geopolitical, insider, and disruptive-passenger risks, with contributions from ASIO and senior airline risk leaders.

The Performance-Based Security Oversight segment reflected the growing momentum toward adaptive, data-driven regulatory approaches. Discussion centred on Security Management Systems (SeMS), digital trust mechanisms, and the potential of Aviation Security Trust Frameworks using verifiable credentials to streamline oversight and strengthen cross-sector assurance.

Overall, the event reinforced the need for harmonized global action, deeper collaboration between states and industry, and continued innovation in security governance. The participation of major airlines, regulators, and security agencies demonstrated broad commitment to strengthening aviation's protective posture and advancing practical pathways toward more integrated, risk-based security management.

7.3 Safe Skies Forum 4 (Marrakesh, Morocco) – April 2025

IATA participated in the Fourth Safer Skies Forum held in Marrakech in April 2025, representing the interests of our member airlines and the Geopolitical Risk Task Force (GRTF). Throughout the three-day forum, IATA engaged with States, international organizations, regional partners, and operational stakeholders to reinforce the industry's priorities for conflict-zone risk management and civil–military coordination.

IATA's presence ensured that airline operational realities were clearly conveyed, particularly regarding the urgent need for timely and consistent State-issued information during rapidly evolving geopolitical events. IATA emphasized that while operators must ultimately determine their own risk tolerances, States hold the responsibility for providing authoritative, high-quality intelligence related to conflict-zone activity, missile testing, GPS interference, and airspace closures. This message resonated strongly across the discussions and was reflected in the forum's concluding themes.

From a GRTF perspective, IATA stressed the value of deeper regional collaboration, particularly in areas where State-to-State information sharing remains inconsistent or siloed. IATA reinforced industry's willingness to support joint contingency planning and participate in regional early-warning mechanisms, if States commit to transparency and timely dissemination of verified information.

Overall, IATA's participation ensured that the airline perspective remained central to the dialogue and that the forum's recommendations reflected practical, operationally realistic requirements. Our contributions helped advance momentum toward a more harmonized, predictable, and safety-focused global framework for managing the risks of operating near conflict zones.

https://tc.canada.ca/en/initiatives/safer-skies-initiative/fourth-safer-skies-forum-report

7.4 World Cargo Symposium (Dubai, UAE) – April 2025

A dedicated session on air cargo security was incorporated into the WCS Safety and Security Stream, which included a presentation by Cathay Cargo followed by a Panel discussion. Increasing awareness of the overlaps between security and safety featured prominently during discussions. PLACI alignment and CSD/eCSD reform were also discussed.

7.5 IID Workshop (Dubai, UAE) – April 2025

On 14 April, on the sidelines of World Cargo Symposium, IATA held a dedicated Workshop covering the recent Improvised Incendiary Device (IID) incidents, attended by 30 experts from various airlines. The workshop canvassed the IATA-led response so far, ICAO/policy updates and ongoing challenges and impacts. Following these discussions, a set of priorities were agreed to guide IATA's advocacy efforts.

7.6 IATA-UPU Contact Committee Meeting (Dubai, UAE) – April 2025

IATA participated in the provided an update on airmail security provided an update on the status of carriers regarding new security measures for mail transported by air and an overview of the CSD/e-CSD reform initiative.

7.7 CSD/eCSD Reform Workshop (Madrid, Spain) – May 2025

On 13 May, IATA, in collaboration with the Cargo Security Working Group (CSWG), hosted a Consignment Security Declaration (CSD) Workshop in Madrid to advance the ongoing CSD/e-CSD reform initiative. The event

brought together 27 industry experts representing airlines, freight forwarders, postal operators, IATA, and the Universal Postal Union (UPU). To complement the reform priorities previously identified at the last reform workshop in 2023, several additional priorities and outcomes were identified to guide the next phase of the reform. A total of around 40 priority areas were agreed.

7.8 IATA-UPU-ICAO Webinar (Online) – May 2025

The joint IATA-UPU-ICAO webinar, attended by almost 1000 guests explored trends, regulations and collaborative strategies to boost security and combat crime in the postal system, including a presentation on security in airmail by IATA. The webinar highlighted the importance of our collaboration and industry-government partnership to ensure the postal system remains safe and secure.

7.9 Beijing Liaison Visit Mission – May 2025

Conducted a series of high-level engagements in Beijing focused on advancing risk-based aviation security and management system implementation. This included delivery of a dedicated workshop on Security Management Systems (SeMS), SeMS Certification, and conflict-zone risk management, supported by full simultaneous interpretation to ensure broad stakeholder participation.

The mission also included participation in a regional workshop on SeMS, and geopolitical risk hosted by the Civil Aviation University of China, as well as briefings with the China Air Transport Association (CATA). These activities strengthened regional understanding of performance-based security oversight, promoted alignment with international best practices, and reinforced cooperation between industry, academia, and national stakeholders on emerging geopolitical and operational risks.

7.10 IATA Cargo Experts Conference (Brussels, Belgium) – September 2025

The Cargo Experts Conference featured dedicated sessions on air cargo security, including a panel discussion exploring both the opportunities and challenges of digitizing cargo security processes, using the CSD as a case study and a presentation on aviation cyber security with a focus on air cargo and supply chains.

7.11 Follow-up CSD/eCSD Reform Workshop (Brussels, Belgium) – September 2025

The reform working group collated and reviewed action items and priorities from prior workshops and meetings into four key categories. These agreed outcomes were used to guide the first draft of the reform package.

7.12 Aviation Security Forum (Montreal, Canada) – November 2025

The session saw the attendance of over 55 participants from key aviation industry stakeholders gathering at IATA's Montreal office. The Forum and SeMS Workshop drew participants from airlines, international organizations, and external service providers (ESPs) representing various geographic regions. This year's Forum focused on the ongoing and growing challenges arising from geopolitical complexities and tensions. From airspace closures arising from economic and political sanctions, civil wars and military operations, to the weaponization of drones, the ever-shifting geopolitical landscape has been challenging for the civil aviation industry and regulatory partners to navigate. The forum focused discussion amongst participants on the key

challenges in the effective execution and implementation of Threat Assessment and Risk Management processes in attempting to prepare for and minimize the impacts of such geopolitically related disruptions to civil aviation operations.

The fourth iteration of the IATA SeMS Workshop was aimed at the continuous development and evolution of SeMS as not only being a mandatory requirement for IATA by virtue of the IATA Operational Safety Audit (IOSA) but also being able to be adopted by other aviation industry stakeholders for functional and practical use. The theme for the SeMS Workshop, in alignment with the overall theme of the Forum itself, cantered around the core SeMS element of Threat Assessment and Risk Mitigation and drew robust discussions on the challenges and potential in developing related Security Performance Indictors (SePIs) in the benchmarking of the implementation of Security Management Systems (SeMS). This provided a further opportunity for participants in (re)evaluating their current practice of SeMS, and for other organizations not yet practicing SeMS, promoting and facilitating the adoption of SeMS.

The aim of the ongoing IATA SeMS Workshops is to support IATA SeMS Strategy promotion and implementation of SeMS to provide a more consistent and standardized structure that facilitates effective, efficient and more uniform security standards throughout the aviation industry through collaborative industry engagements between key aviation stakeholders.

7.13WGACS (Bern, Switzerland) – November 2025

IATA attended the ICAO Aviation Security Panel Working Group on Air Cargo Security (WGACS) between 5-7 November 2025 in Bern. IATA is a key member of the WGACS, which consists of ICAO Member States and other aviation trade associations. The WGACS overall mandate is to enhance global air cargo security and to align air cargo security policies, standards, measures, and guidance material.

WGACS members complemented IATA's IID Guidance document and noted the value that the guidance has provided to industry members. ICAO.

IATA provided an update on the CSD/e-CSD reform initiative to the WGACS, including an overview of the key proposed adjustments and the project timeline. IATA requested assistance and feedback from WGACS members to help guide the reform initiative, with bilateral State outreach to commence shortly.

Other topics discussed during the WGACS meeting included:

- Airmail security
- Status of new technologies for screening air cargo and mail
- Unmanned aircraft
- Supply Chain regulated entities (Regulated Agent and Known Consignor)
- Ongoing response to the IID sabotage incidents

The meeting highlighted once again the value of industry-government-association partnership in our shared goal of protecting and securing global air cargo and supply chains.

7.14 2nd IATA-UPU Contact Committee Meeting (Bern, Switzerland) – November 2025

At the 2nd IATA-UPU Contact Committee meeting, IATA provided an overview of the revised IID Guidance document, highlighting the mail security components. An update on the CSD/e-CSD reform was also provided.

7.15 WCO SAFE Working Group (Brussels, Belgium) – November 2025

IATA, with the New Zealand Customs Service and the United Kingdom Revenue and Customs, participated in a panel discussion on the ongoing relevance of the WCO SAFE Framework of Standards in facilitating and securing trade. The discussion highlighted the need for harmonized standards to support advanced risk assessment mechanisms based on cargo data, as well as the critical importance of global inter-agency partnerships to prevent duplicative or conflicting reporting requirements across international supply chains.

7.16 Inflight Theft Workshop (Doha, Qatar) – December 2025

In response to growing concerns around in-flight theft affecting international air carriers, IATA and Qatar Airways organized a closed workshop designed to foster collaborative risk-based solutions under legal confidentiality provisions. The workshop was hosted by Qatar Airways and provided an opportunity to build trust, exchange sensitive operational insights, identify practical mitigation strategies and recommended practices that can be shared with the broader IATA membership of airlines.

- The workshop brought together international carriers to address the growing threat of in-flight theft, sharing sensitive operational insights and agreeing with the need for a unified, industry-wide approach to mitigation and prosecution of offenders.
- Participants confirmed that in-flight theft is often organized, transnational, and conducted by coordinated groups whose behaviours follow identifiable pre-flight, gate, and in-flight patterns.
- Airlines identified a range of practical mitigations spanning crew training, behavioural detection, passenger awareness, SOP refinement, post-incident handling, and improved data reporting—to strengthen prevention, detection, and response.
- Significant legal and regulatory gaps were highlighted, including major barriers to cross-border data sharing, uneven adoption and application of the Montreal Protocol 2014 (MP14), and inconsistent recognition of airlines as complainants by law enforcement.

The workshop agreed on clear next steps: development of an industry guidance document, creation of a common taxonomy and anonymized dataset, coordinated advocacy for MP14 ratification and prosecutorial pathways, and alignment through IATA's Security Advisory Council (SAC) and GADM/IDX mechanisms.

8 Products, Training and Services

IATA Security Training – Summary Highlights 2025

2025 marked a year of steady activity for IATA Security Training, with sustained demand across key security areas. The industry's increased focus on operational resilience, airspace risk, and structured security management continued to drive strong participation.

- Airspace Security and Risk Assessment training maintained strong momentum, with more than 130 professionals trained as organizations strengthened their capabilities in conflict zone and geopolitical risk assessment.
- The SeMS Certification Program continued to grow, with around 180 employees completing the SeMS Introductory Course. Advanced SeMS training remained a core offering, reaching over 150 participants from airlines, airports, CAAs, and other partners.
- Foundational security capabilities continued to expand, with Aviation Cyber Security and Security Audit & Quality Control attracting a broad and diverse audience across regions and sectors.
- The Abu Dhabi Training Center completed its first full year, positioning itself as a key regional hub and expanding access to IATA's security training portfolio across the Middle East.

IATA's diploma programs remained a trusted pathway for professional advancement. Both the Aviation Security Management Diploma and the Aviation Cyber Security Management Diploma continued to attract security professionals seeking structured, progressive development, reinforcing the industry's confidence in IATA's long-term training framework.

Overall, 2025 underscored the sector's continued commitment to strengthening integrated security management, cyber resilience, and airspace risk awareness—while reaffirming IATA's role as a trusted partner in advancing the aviation security workforce.

Security Management System Manual 2025

- 2025 was a record-breaker for unique customers, with 158 different groups or companies choosing the SeMS manual.
- Highest number of purchased units in 2025, equalling record number in 2023.
- Asia Pacific and Middle East regions have increased their adoption of the manual by 5% since inaugural released in 2018.

9 Looking Forward

From Frameworks to Front-Line Protection

After several years of rapid policy development and analytical work, 2026 marks a decisive shift from design to delivery for aviation security and risk management. A series of major initiatives matured in parallel during 2024–2025—covering airspace risk management, GNSS resilience, performance-based oversight, and digital trust in security information-sharing. In 2026, these frameworks move into operational implementation across airlines, regulators, and air navigation service providers.

This transition reflects both necessity and readiness. Escalating geopolitical volatility, multi-domain threats, and navigation disruption have made theoretical alignment insufficient. At the same time, industry and authorities now share common methodologies, tools, and governance models capable of supporting consistent execution at scale.

The year ahead will be defined by embedding these initiatives into daily operational decision-making: strengthening civil–military coordination, enabling real-time situational awareness, formalizing risk-based oversight, and improving resilience to emerging threats. Together, these measures will help sustain the high levels of safety and security achieved by civil aviation, while ensuring that the system remains adaptable in an increasingly unstable global environment.

Aviation Security Trust Framework (ASTF) | https://astf.iata.org

In 2025, IATA advanced the Aviation Security Trust Framework (ASTF) as a foundational enabler for modern, performance-based aviation security oversight. ASTF provides a secure digital trust layer that allows regulators and industry partners to verify aviation security information using cryptographically verifiable credentials, without requiring system-to-system integration or broad data sharing. The framework supports ICAO Annex 17 concepts such as Aircraft Operator Security Programs (AOSPs), Supplementary Station Procedures (SSPs), and Security Management Systems (SeMS), enabling States to recognise equivalent measures and reduce duplication of oversight activity.

ASTF strengthens confidence in cross-border security arrangements by ensuring authenticity, integrity, and provenance of shared security data, while preserving national sovereignty and operator control of information. By shifting from document-based exchanges to trusted digital assurance, ASTF enhances transparency, supports risk-based decision-making, and improves the efficiency of regulatory coordination. In an increasingly complex threat environment, ASTF represents a key step toward scalable, resilient, and globally harmonized aviation security governance.

Implementation of the EASA–IATA GNSS Interference Mitigation Plan (2026)

In 2026, the joint EASA–IATA framework to mitigate Global Navigation Satellite System (GNSS) interference moved from policy alignment into operational implementation. States, ANSPs, and airlines began embedding standardized GNSS disruption reporting into safety and security management systems, improving the consistency and timeliness of incident data. Airspace users expanded contingency procedures for navigation outages, including greater reliance on alternative navigation sources, revised approach minimum, and enhanced crew training for degraded PNT environments.

Civil–military coordination mechanisms were strengthened to improve situational awareness of intentional and unintentional interference, enabling more proactive risk mitigation and targeted advisories. Infrastructure resilience also advanced through increased monitoring of interference hotspots and the prioritization of backup navigation capabilities in high-risk regions.

Together, these measures marked a shift from reactive response to structured resilience. GNSS disruption is now treated as a systemic, multi-domain risk rather than a localized anomaly, reinforcing the need for sustained international coordination and continuous operational adaptation across the global aviation system.

Implementation of ITOP 2.0 and the IATA Liaison Desk (2026)

In 2026, IATA transitioned the IATA Liaison Desk and the IATA Tactical Operations Portal (ITOP) 2.0 from concept into full operational implementation, strengthening real-time coordination between airlines and the U.S. FAA Air Traffic Control System Command Center. The modernized platform replaced legacy infrastructure with a secure, internally managed system supporting live operational communication, structured event management, and integrated business intelligence.

ITOP 2.0 enabled airlines to access near-real-time airspace status, contingency updates, and validated State and ANSP information through a single trusted interface. A standardized event lifecycle ensured that emerging disruptions—such as airspace closures, conflict-related activity, cyber incidents, or ATC degradation—were verified with authoritative sources before dissemination.

Through centralized coordination and regional integration, ITOP 2.0 improved predictability, strengthened situational awareness, and supported airline decision-making during operational and geopolitical disruptions. This marked a shift from reactive coordination to a digitally enabled, risk-informed model for global airspace contingency management.

Implementation of GRTF Airspace Security Guidance (Version 2) | 2026

In 2026, IATA released Version 2 of the GRTF Airspace Security Guidance as an operational tool to support airlines in managing conflict-zone and militarized airspace risks through structured, defensible processes. Developed by the IATA Geopolitical Risk Task Force (GRTF), the guidance moved beyond high-level principles toward practical implementation, emphasizing continuous threat identification, intent-and-capability assessment, and risk-based decision-making integrated with Safety and Security Management Systems (SMS/SeMS).

Airlines adopted the guidance to formalize governance arrangements, strengthen intelligence validation, and document routing decisions—particularly when operating near prohibited or high-risk FIRs and within Free Route Airspace environments. New focus areas, including buffer-zone justification, point-of-no-return logic, and performance indicators, improved transparency and auditability of conflict-zone decisions.

Version 2 reinforced the industry's shift from reactive avoidance to systematic airspace risk management, helping ensure that operational flexibility is matched by accountable oversight and that civil aviation is protected from both deliberate and inadvertent military threats.

Aviation Security Forum 2026

The next Aviation Security Forum will be held in Madrid, Spain from 09 – 12 November 2026.

More details to come.

10 Strategic Partner Contributions

10.1 Dragonfly from Dow Jones – Navigating a Multisphere World

The strategic outlook for 2026 offers little respite from volatility for the aviation sector, as zones of stability contract and contested regions expand. We enter the year with conflict risks rising almost everywhere, and with it the potential for contagion, political crises and sudden policy changes, and supply chain disruption.

Geopolitical competition is playing out across all domains, from politics and economics, to trade, cyberspace, space and our societies. This is driving a multitude of risks that the aviation sector is exposed to including military conflict, hybrid warfare, GPS interference, contentious politics and activism – to name a few.

These issues will almost certainly contribute to persisting and evolving challenges around safety, security, reputation and business continuity for airlines in 2026, and indeed over the coming years.

The threat of hybrid warfare

The intensification of hybrid warfare in 2025 is very likely to continue into 2026 as geopolitical tensions remain unresolved. Hybrid, or 'grey-zone', warfare conducted below the threshold of open conflict, is becoming a defining feature of a global system stretched by unresolved conflicts. It blurs red lines, shifts front lines, weaponises trade and infrastructure, and replaces deterrence by clarity with deterrence by uncertainty. Watching for the pressure points of grey zone testing, probing and provocation that could trigger escalation will be vital throughout 2026.

The use of drones and the measures taken to limit the disruption they cause are likely to remain a key consideration for air safety and route planning for airlines. These cheap systems are designed to evade detection and have prompted restrictions to airspace and sporadic airport closures in eastern and northern Europe. Tactical and technical innovation in this area by hostile actors will demand continuous innovations in security and resilience to mitigate the threat.

Indeed, the disruption caused by drones in Europe shows no signs of abating. As the war between Russia and Ukraine continues, Moscow seems intent on imposing a cost on Europe for its support to Kyiv. European officials have suggested that Russia is behind the spate of drone incidents that have affected European airports and warned of the threat posed by Russian hybrid tactics. The head of the UK's Civil Aviation Authority said in November that 'it's not a question of if, only of when' that 'organised' drone attacks disrupt UK airports. Recent cases of suspected drone launches from ships in Russia's shadow fleet highlight that few areas are out of range from such disruption.

The shift towards global militarisation

While multilateral diplomacy, aid and international cooperation are in retreat, political, economic and security systems are straining beyond their limits — and global power is decisively shifting towards militarisation. Global defence spending reached a record $2.7 trillion in 2024, which is about 13 times total development aid. Investing in warfighting capabilities eclipses investments in stability and development, which is a global trend that shows no sign of reversing any time soon.

Global and regional powers are investing heavily in advanced military capabilities and using them more assertively to pursue their interests. At the same time, guardrails against armed conflict are being dismantled. Support for development aid and multilateral diplomacy is waning, while institutions designed to prevent and mitigate wars are log-jammed or face declining credibility. With fewer mechanisms to de-escalate crises, 2026 is likely to bring rising friction between states and deeper fragmentation of the international system, and with it increased geopolitical risk.

Military coercion is also displacing multilateral diplomacy as the norm of statecraft. Russia's continued assault on Ukraine, the US and Israel's pre-emptive strike on Iranian nuclear facilities in June 2025, and China's assertive posture in the

South China Sea all illustrate a willingness to sidestep international law and long-standing norms. If left unchallenged, such behaviour will probably embolden others, eroding non-intervention principles and reinforcing a more anarchic global order.

For the businesses, including the aviation sector, the impact is profound. A world of increasingly assertive hard power means heightened exposure to volatility, policy-driven disruption and strategic uncertainty. Resilience will depend on agility: monitoring flashpoints, anticipating behaviour outside traditional norms and stress testing against scenarios in which deterrence fails.

The above is adapted from Dragonfly's annual report: Strategic Outlook 2026: A Multisphere World. Strategic Outlook is Dragonfly's annual global risk intelligence estimate. Its purpose is to provide decision-makers with a forward-looking and actionable assessment of geopolitical and global security risks in the year ahead. Download your copy here.

10.2 CEIA S.p.A

CEIA is a company dedicated to the development, design and manufacturing of electromagnetic inspection systems. With over 55 years of experience, our company has established itself as a global leader in threat electromagnetic detection technologies. Design and manufacturing of our product range is done 100% in-house so we maintain a leading position by consistently introducing cutting-edge technology designed to enhance security measures while maintaining efficiency and ease of use. Our activities span research, engineering, and global support for a diverse portfolio of threat detection technologies across various sectors including public venue security, protection of critical infrastructures and aviation security where we are well-known for our advanced screening solutions for both passengers and cargo.

Passenger Screening Solutions

CEIA's product portfolio for passenger screening is extensive, encompassing a range of systems that meet the highest standards of security while ensuring a smooth and fast experience for travellers. Our passenger screening solutions are designed to detect a wide range of potential threats, from weapons and explosives to other prohibited items. Our systems are designed to maximize both security and throughput making CEIA's solutions a reliable choice especially for high-traffic airport checkpoints.

- **Walk-Through Metal Detectors (WTMD):** For decades, our WTMD models have been central to airport security checkpoints. They offer multi-zone detection capable of pinpointing threats on a passenger's body, including items hidden within cavities. Engineered for high discrimination, they detect metallic threats while ignoring common personal items like glasses, belts and jewellery to reduce nuisance alarms.
- **Shoe Analyser:** Our model, the **SAMDEX,** automatically detects both metallic threats and explosives concealed within footwear. It enables passengers to be screened without removing their shoes, significantly increasing the checkpoint's throughput and passengers' experience.
- **Liquid Explosive Detection (LEDS):** For 15 years, our models, the **EMA** series, that combine several technologies, have been the preferred solution by airports for screening bottled liquids, aerosols and gels. Certified by several AVSEC authorities, our LEDS can screen various container materials—including plastic, glass, ceramic and metal—without requiring the container to be opened.
- **Security scanner: JANUS**, our brand-new product, is an ultrabroadband enhanced security scanner aimed at the inspection of passengers for the automatic detection of metallic and non-metallic threats concealed under clothing. Thanks to its unique technology, the scanner also allows for the automatic detection of metallic threats within body cavities and shoes.

Cargo Security Screening Solutions

For air cargo industry, CEIA provides specialized electromagnetic inspection systems that prioritize speed and accuracy without the need for human intervention.

The **EMIS** series scanners are designed for the automatic detection of IEDs inside non-metallic cargo. They are particularly effective for screening commodities such as perishable goods, chemicals, printed material and textile where traditional method based upon X-ray imaging tend to be difficult and less efficient.

The series currently includes models for different throughput needs with systems adapted for rapid package screening and larger ones for screening entire pallets.

Unlike traditional X-ray systems, the EMIS series uses electromagnetic analysis to automatically signal threats, allowing handling operations to improve both security and efficiency.

Overview

CEIA has established itself as a trusted leader in aviation security, particularly in the areas of passenger and cargo screening solutions. By combining cutting-edge technology, reliability, and ease of use, the company provides a broad portfolio of products that enhance both the security and efficiency of global aviation operations. From walk-through metal detectors to cargo metal detectors, CEIA's solutions ensure that aviation security professionals have the tools they need to prevent threats and maintain both passenger and cargo safety and security.

As aviation security continues to evolve, CEIA remains committed to advancing its offerings to meet the growing demands of the industry.

Key Activities and Global Reach

- **Integrated R&D and Manufacturing:** CEIA maintains a 100% in-house production model, ensuring that all hardware and software components are engineered for total compatibility. This includes operating an ISO 17025 accredited laboratory for electromagnetic compatibility and human exposure testing.
- **Compliance and Training:** The company's activities include providing extensive training and certification programs for the use and maintenance of its equipment, ensuring airport operators remain compliant with evolving international regulations.
- **Networking and System Management:** CEIA offers advanced networking software solutions that allows to monitor and collect statistical data across our entire fleet of aviation security screening solutions.
- **Global Event Support:** Beyond aviation, CEIA is also very active in securing major international events and large public venues such as stadia and sports arenas, concerts, expo and various global summits, demonstrating the high scalability of our airport-grade technology.

10.3 Ground Controls – When Borders Learn to Think in Movement, Not Moments

For years, progress in aviation security has been measured in milliseconds.

Shorter queues. Faster identity checks. Cleaner biometric matches. These gains are real, and they matter. They have made borders more predictable, more scalable, and often more humane. But speed has also become a convenient proxy for success. One that quietly obscures a deeper limitation.

Borders have become very good at answering the question *"Who is this person?"*
They are still struggling with *"What does this movement mean?"*

That distinction is no longer academic. It is operational.

Every day, travellers arrive who satisfy every formal requirement. Their documents are valid. Their

biometric checks pass. Their API and PNR records raise no flags. And yet, in hindsight, some of these journeys will later be understood as part of something larger. Activity that only became visible when viewed across time, associations, and repeated movement.

Risk, in other words, rarely announces itself at a single checkpoint.

It accumulates. It drifts. It hides in patterns that only emerge when identity, intent, and context are interpreted together. It is where the limits of checkpoint-centric thinking become apparent.

The industry has begun to sense this shift, even if it has not always named it directly. We speak more frequently now about intelligence-led borders, advanced analytics, and interoperability. But beneath the terminology lies a more consequential transition: a move away from borders as transactional control points, toward borders as intelligence systems.

Many existing risk models still struggle with this transition.

They treat data inputs as independent signals. A watchlist hit increases risk. An itinerary anomaly increases risk. A prior overstay increases risk. Each of these may be true. None of them, on their own, explains very much. Risk is not additive; it is relational.

What matters is how signals intersect. How journeys repeat or subtly evolve. How associations form across datasets. How movement aligns with patterns authorities already know to matter but rarely see early enough. Without this relational layer, even rich data streams remain fragmented. Informative, but incomplete.

It is where interoperability becomes decisive, and where it is most often misunderstood.

Technical interoperability, the ability for systems to exchange data, is necessary but insufficient. The harder challenge is operational interoperability: ensuring that shared data leads to shared understanding, without flattening the distinct missions of different authorities. Immigration services, aviation security, customs, and law enforcement do not define risk in the same way, nor should they.

True interoperability respects those differences. It allows intelligence to be interpreted through mission-specific lenses, while remaining anchored in a common analytical foundation.

In practice, this demands a shift in how passenger risk is conceptualized.

Rather than static profiles tied to individual journeys, risk must be treated as **dynamic movement intelligence**. Profiles evolve as new information arrives. Context deepens. Signals gain or lose relevance over time. The system does not merely flag anomalies; it reasons about behaviour.

This shift also reframes facilitation.

When risk is understood contextually, most travellers move faster, not slower. Low-risk passengers are cleared with greater confidence. Resource management is optimized: attention is reserved for situations where patterns genuinely justify scrutiny. Security and efficiency stop being competing objectives; they become parallel outcomes of better intelligence.

None of this diminishes the role of human judgment. On the contrary, it makes it more central.

Experienced professionals at borders bring context, intuition, and accountability that no system can replace. The role of advanced platforms is not to decide on their behalf, but to support better decisions earlier, by reducing noise, surfacing meaningful patterns, and explaining *why* something matters, not just that it does.

As conversations around digital identity, data sharing, and privacy intensify, including initiatives such as One ID, this balance will become increasingly important. The future of passenger risk assessment will not be defined by how much data is collected, but by how responsibly and intelligently it is interpreted.

The aviation community now stands at a quiet inflection point.

The technical tools exist to move beyond identity checks and isolated intent signals. What remains is

a collective willingness, across governments, airlines, and technology partners, to rethink borders not as moments of control, but as **continuous systems of understanding**.

At Ground Controls, this perspective has shaped years of work alongside authorities grappling with exactly this challenge: how to see earlier without acting harder, how to connect signals without overwhelming operators, and how to preserve sovereignty while embracing analytical depth. It is a philosophy born less from theory than from lived operational reality.

Those who make this shift will not simply build faster borders.
They will build borders that understand movement, predict risk patterns, and in doing so, make security not just more efficient, but more intelligent.

11 Glossary

A42	Assembly 42nd Session
ANSP	Air Navigation Service Provider
AOSP	Aircraft Operator Security Programme
API	Advanced Passenger Information
ASTF	Aviation Security Trust Framework
ATC	Air Traffic Control
AVSECP	Aviation Security Panel
CAAs	Civil Aviation Authorities
CCTV	Closed-Circuit Television
CSD	Consignment Security Declaration
CSWG	IATA Cargo Security Working Group
EASA	European Union Aviation Safety Agency
EC	European Commission
ESPs	External Service Providers
EU	European Union
FAA	Federal Aviation Administration
ICAO	International Civil Aviation Organization
IED	Improvised Explosive Device
IDX	IATA Incident Data Exchange
IID	Improvised Incendiary Device
IOSA	IATA Operational Safety Audit
ITOP	IATA Tactical Operations Portal
GADM	Global Aviation Data Management
GNSS	Global Navigation Satellite System
GRTF	Geopolitical Risk Task Force
LBA	Luftfahrt Bundesamt
LEDS	Liquid Explosive Detection
MP14	Montreal Protocol 2014
NOTAM	Notice to Air Mission/Airmen
OSS	One Stop Security
PNR	Passenger Name Record
PNT	Positioning, Navigation, and Timing
PPBM	Positive Passenger/Bag Match
RoE	Recognition of Equivalence
SAC	Security Advisory Council
SAGAS	Stakeholders' Advisory Group on Aviation Security
SeMS	Security Management System
SePIs	Security Performance Indicators
SOP	Standard Operating Procedure
TSA	Transportation Security Administration
UAE	United Arab Emirates
UK CAA	United Kingdom Civil Aviation Authority
UN	United Nation

UPU	Universal Postal Union
WCO	World Customs Organization
WGACS	Working Group on Air Cargo Security
WP	Working Paper
WTMD	Walk-Through Metal Detectors