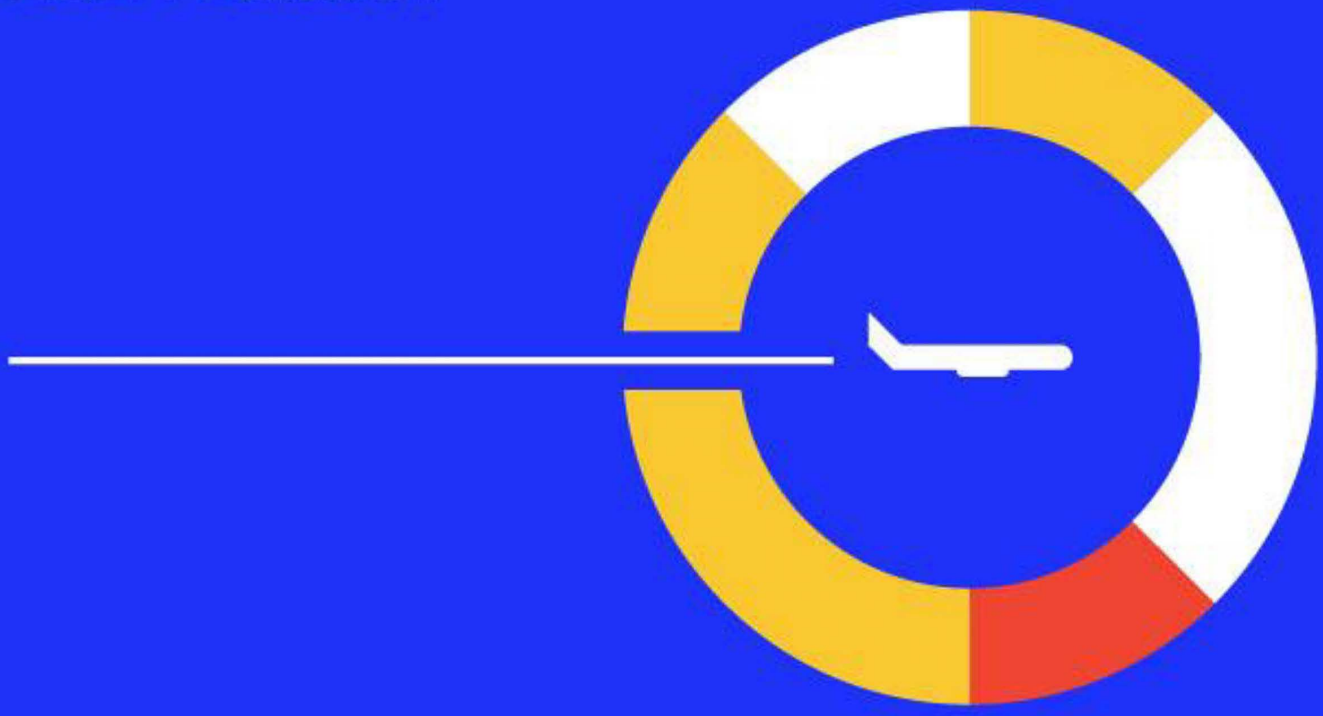
IATA Annual Security Report

2024 Edition



Contents

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.

Supported by our Strategic Partners

Nuctech Company Limited (Nuctech) is an advanced security & inspection solution supplier in the world. Committed to innovation and tailored offerings, Nuctech serves as a reliable security solution and service supplier in over 160 countries and 400 airports/air cargo facilities worldwide. With 20 global service depots and 5 factories, we strive to enhance global civil aviation security. We work closely with airports of all sizes to create bespoke security programs that cater to their evolving needs.

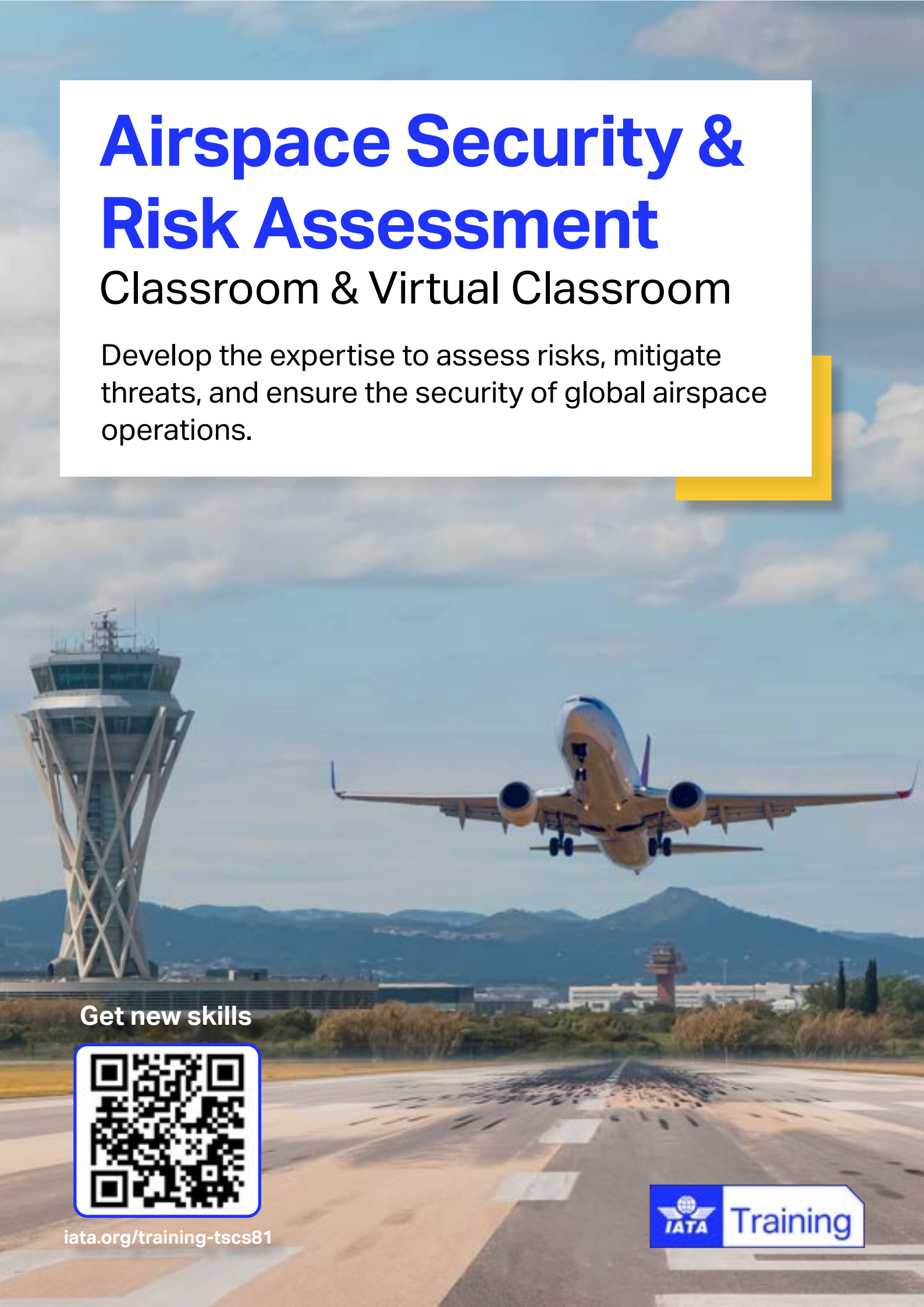
As a responsible high-tech enterprise, Nuctech focus on the security domain and devotes itself to becoming the leader in the global security market. Nuctech enhances the customers' value with the ever-ongoing innovation, feeding back the society by creating more advanced security products, solutions, and service.

Strategic Outlook 2025: The Grey Swan Problem is Dragonfly's annual strategic intelligence estimate for those whose decisions hinge upon an understanding of emerging geopolitical and strategic security risks.

Airspace Security & Risk Assessment

Classroom & Virtual Classroom

Develop the expertise to assess risks, mitigate threats, and ensure the security of global airspace operations.



Get new skills

iata.org/training-tscs81

IATA Training

1. Glossary of Terms

Acronym	Description
A4A	Airlines for America
AI	Artificial Intelligence
AOSP	Aircraft Operator Security Program
ARF	Aircraft Recovery Forum
ASAC	Aviation Security Advisory Committee (TSA)
ASPAC	Asia Pacific
ASTF	Aviation Security Trust Framework
AUI	Act of Unlawful Interference
AVSEC	Aviation Security
AVSECFAL	Aviation Security Facilitation
AVSECP	Aviation Security Panel
BCAS	Bureau of Civil Aviation Security
B2B	Business to Business
B2C	Business to Consumer
BoG	Board of Governors (IATA)
BOI	Bureau of Immigration
CCT	Contingency Coordination Team
CGO	Cargo Operations (part of the IOSA scope)
CRMWG	Cyber Management and Resilience Working Group
CSD	Consignment Security Declaration
CSSA	Cybersecurity for Security, Safety and Airworthiness (IOSA)
CSWG	Cargo Security Working Group
DG-ARM	Director General – Analytics & Risk Management
DG MOVE	The European Commissions Directorate General Mobility and Transport
DID	Decentralized Identifiers
EASA	European (Union) Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
EFG	European Focus Group
EGRICZ	Expert Group on Regional Conflict Zones
ERP	Emergency Response Planning
ESP / ESPs	External Service Provider / s
EU	European Union
EUROCAE	The European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration (USA)
GASeP	ICAO Global Aviation Security Plan
GNSS	Global Navigation Satellite Systems
GRH	Ground Handling Operations (part of the IOSA scope)
GTRF	Geopolitical Risk Task Force
IATA	International Air Transport Association
IASeR	IATA Annual Security Report

ICAO	International Civil Aviation Organization
IDX	Incident Data eXchange (IATA)
IED	Improvised Explosive Device
IID	Improvised Incendiary Device
IOSA	IATA Operational Safety Audit
IRAG	Integrated Aviation Security Risk Assessment Group (EU)
IRM	Integrated Risk Management
IRRM	Integrated Risk and Resilience Management
IOSA	IATA Safety Audit Program
ISARPs	IOSA Standards and Recommended Practices
ISM	IOSA Standards Manual
ITOP	IATA's Tactical Operations Portal
JMSB	John Molson School of Business
KCs	Known Consignors
KPIs	Key Performance Indicators
LAGs	Liquids, Aerosols and Gels
NCASP	National Civil Aviation Security Program
NOTAM	Notice to Airmen
OEM	Original Equipment Manufacturers
ORG	Organisation (scope of IOSA)
OAC	Operations Advisory Committee
OSS	One Stop Security
PLACI	Pre-Loading Advance Cargo Information
RAs	Regulated Agents
RoE	Recognition of Equivalence
RTCA	Radio Technical Commission for Aeronautics
SAC	Security Advisory Council
SEC	Security (part of the IOSA scope)
SeMS	Security Management System
SECTF	SEC Task Force
SP	IATA Strategic Partners
SSCC	Safer Skies Consultative Committee
SSP	Supplementary Station Procedures
TFP	Trust Framework Panel (ICAO)
TSA	Transportation Security Administration (USA)
UAV	Unmanned Aerial Vehicle
UN	United Nations
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UNSCR	United Nations Security Council Resolution
USAP	Universal Security Audit Programme (ICAO)
VC	Verifiable Credentials
W3C	World Wide Web Consortium
WGACS	Working Group on Air Cargo Security (ICAO)

WGTR	Working Group on Threat and Risk (ICAO)
WSOC	World Safety and Operations Conference (IATA)

Foreword

It is with great pleasure that we present the 2024 IATA Annual Security Report (IASeR), an in-depth reflection of our collective efforts in ensuring a secure and resilient air transport industry for all. This year has seen an evolving landscape of challenges, from emerging threats to longstanding risks that require innovative approaches and dedication to compliance.

This annual readout has been developed taking note of IATA's own publicly available assessment of risk in 2025: Heightened Policy Uncertainty and own IATA's Annual Review 2024.

We had initially finalised a draft prior to the tragic and unacceptable events involving Azerbaijan Airlines Flight 8243. As a result, IATA released an important statement.

The industry has been incredibly resilient navigating against these complexities by fostering a culture of oversight, continuous improvement and enhancing industry to government partnership and collaboration.

The continued adoption of a security management system approach has been rigorously tested and continuously improved to ensure we remain ahead of potential risks, particularly in the face of an increasingly interconnected world.

Throughout the year, industry has prioritized not only the safeguarding of physical and digital assets but also the well-being of people. The resilience shown by airline employees, partners, and stakeholders has been critical to maintaining our operational integrity during times of uncertainty.

This report highlights the key security initiatives, achievements, and lessons learned over the past year, offering transparency into the strategies that have allowed IATA and its member airlines to play a vital role in mitigating threats effectively.

We are proud of the work our security teams have done, and the progress made. However, we remain acutely aware of the evolving nature of security risks and are committed to continuous improvement to face future challenges.

As we look ahead, our collective focus will remain on strengthening our security posture through proactive risk management, leveraging policy reform, and maintaining a deep sense of responsibility for the safety and security of civil aviation.

Thank you to all who have contributed to making this year a success.

Matthew Vaughan

Director, Aviation Security

2. Executive Summary

The 2023 IATA Annual Security Report (IASeR) was the inaugural version and provided end-to-end perspective in terms of aviation security policy, risk, and regulations.

The 2023 report was structured around five key areas of interest: **Cybersecurity**, **Civil Protests and Supply Chain Risks, Natural Disasters and Pandemic Risks, Aviation Security Evolution and more broadly, Challenges and Opportunities.**

To some degree, when attempting to reconcile what we expressed with the actual events of 2024, we were not that far off in our estimates.

For this 2024 version, we are focusing on five new areas of strategic interest and opportunity for aviation security professionals to consider. They are presented in no specific order.

- **Second Edition of the Global Aviation Security Plan (GASeP) (DOC 10118) and the Muscat Declaration on Aviation Security and Aviation Cybersecurity** – ICAO has released its second version of the GASeP, which now consists of six key priority areas. The plan itself is directed towards States, but not without the opportunity for industry to recognize the guard rails this provides for all forms of security planning. The success of GASeP adoption is still measured against ICAO's Universal Security Audit Program results, which may not reflect all the improvements implemented by States and industry stakeholders in between audits. Additionally, priority area five focusing on oversight and quality assurance has the potential to influence new thinking by States on current approaches.

- **Geopolitical Risk and Conflict Zones** – The spectre of geopolitical risk continues to disrupt the continuity of civil aviation. We see this being played out in the form of economic sanctions, conflict zones and global navigation systems such as Global Navigation Satellite Systems (GNSS) related spoofing and interference. 2024 has seen interference with civil aviation assets become increasingly indirect or misidentified. Now, more than ever, security and safety must collaborate to navigate risk parameters, define tolerances, and strengthen governance.

  It has reached a point that the IATA Director General (DG) released a press statement on the protection of Civil Aviation from interference – CLICK HERE.

- **Air Cargo Supply Chain** – In the 2023 IASeR, we identified foreign interference as a threat vector of interest. In 2024, the air cargo supply chain, specifically in Europe, experienced a form of this we now refer to as hybrid threats. The regulatory response, comprising mostly of additional security measures, has raised questions about the efficacy of the ICAO Annex 17 baseline.

- **Security Management System (SeMS) Evolution** – 2024 has reaffirmed for us that risk management and regulatory compliance focused on security outcomes are the cornerstones of any good security program. With the onset of hybrid threats, measuring and managing security performance has become more relevant. SeMS represents a positive step for industry ensuring it meets economic mandates and delivery of products and services, while also achieving effective security performance and outcomes.

  In October 2024, IATA issued a press release on the launch of the SeMS Certification Program representing new levels of investment and partnership into this business asset – CLICK HERE.

- **IATA Aviation Security Forum (November 2025)** – We will be hosting the IATA Aviation Security Forum, Montreal, Canada, in November 2025. More information on this event will be released in early 2025.

In addition to the above five key items, several other aviation security issues, and events throughout 2024 deserve a mention:

- Sharp rise and awareness of GNSS spoofing and jamming interference incidents.
- MS804 final report, and its finding that the presence of explosives was on-board.
- Yemen Airlines unlawful aircraft seizure at Sana'a International Airport (June 2024).
- FAA Ruling recommendations for secondary aircraft cockpit door.
- Transport Canada's additional screening for India bound passengers.
- Re-instatement of LAGs restrictions in various jurisdictions (EU).
- CrowdStrike outage (June 2024).
- Numerous airport security breaches resulting in decisions to empty/evacuate airside areas without appropriate risk-based considerations (Cairns, Japan airport).
- Significant number of bomb threats within the Indian civil aviation market.
- Implications for aviation security following the walkie-talkie and pager incidents in Beirut, Lebanon.
- Ontario Supreme Court ruling on PS752.
- Criminal charges handed down in Poland for offences related to Ryanair Flight 4978 (May 2021).

A public article with a UK based counter terrorism business magazine also outlined a few points leading into 2024.

In 2024, the familiar debate resurfaced around the implementation of additional security measures and their near-synonymous association with extraterritorial mandates. At the heart of the discussion lies the industry's growing concern of mandates to implement additional measures based on a threat profile they are often not briefed on and doing so within a compressed timeframe leaving little room for multilateral, pre-decisional consultation.

The industry has long argued that it is equally capable of evaluating, designing, and implementing time-sensitive additional measures to mitigate the intent and capability of emerging threats. Furthermore, there is a need to advocate for a structured plan to revert to baseline measures as soon as practically feasible.

Today's baseline, as we know it, is often a legacy of past additional measures that have become permanent—a phenomenon some likened to a "Stockholm Syndrome" approach to aviation security.

This raises a critical question: what about the unknown? How do we account for threats that are largely unknown or those we cannot fully comprehend?

The challenge remains - to strike a balance between proactive action, and the risk of perpetually evolving the Annex 17 baseline that may eventually hinder operational efficiency and industry adaptability, without consideration for deregulation where possible.

The debate is far from over, but it underscores the need for greater collaboration and transparency in determining and implementing security measures that address not just what we know, but what we cannot yet foresee.

The capacity for industry or regulators to realize this debate often centres on two distinct methodologies: probabilistic and deterministic approaches. Both are valuable, but striking the right balance is imperative for a protective security framework that is both effective and efficient.

The probabilistic approach relies on statistical models and historical data to estimate the likelihood of specific risks.

For example, it might predict the probability of a weapon being smuggled onto an aircraft or assess

the risk of a cyberattack targeting air traffic control systems.

This approach is particularly useful for optimizing resource allocation, focusing efforts where the residual risk is measured to be the most significant.

On the other hand, the deterministic approach operates under the assumption that certain risks will eventuate unless actively mitigated. This method emphasizes preparation for worst-case scenarios, regardless of their likelihood. For instance, a deterministic mindset ensures protocols are in place for handling an aircraft hijacking or GNSS interference—events with potentially catastrophic consequences. While this approach guarantees a robust defence, it can lead to over-preparation, diverting resources to low-probability events at the expense of addressing more pressing risks.

The tension between these methodologies is not merely theoretical. Resource constraints in aviation security demand a pragmatic balance. Overreliance on probabilistic models' risks underestimating high-consequence risks, while a purely deterministic stance can result in inefficiencies and missed opportunities to address likely scenarios.

Both perspectives are necessary, and their integration is essential to address both the likely and the catastrophic nature of risks.

Regulatory frameworks must evolve to embrace this duality. Current international standards often lean deterministic, focusing on compliance and scenario-specific defences. However, there is an increasing recognition of the need for dynamic, data-driven risk assessments that probabilistic methods provide.

The future of aviation security lies in harmonization—leveraging probabilistic methods to prioritize risks and allocate resources efficiently while using deterministic strategies to prepare for worst-case scenarios. This dual approach ensures that aviation systems are not only resilient but also adaptable to emerging threats.

In an age of uncertainty, aviation security professionals must avoid the false choice between likelihood and impact. Instead, the path forward is clear, a balanced, integrated approach that anticipates the probable and safeguards against the catastrophic.

Commit to protecting passengers and airport staff while improving your operational efficiency by following the latest security guidelines with the indispensable IATA Security Management System (SeMS) manual.

Security Management System Manual (SeMS)

- Management (Corporate Commitment, Security Objectives, Security Communication, Change Management, Provision of Resources)
- Documentation (Aircraft Operator Security Program, Security Reporting)
- Aviation Security Quality (Quality Assurance Audits, Quality Control, Security Surveys, Security Tests)
- Security Risk Management (Security Risk Assessment, Threat Identification and Assessment, Risk Management Process)

The **8th edition of the SeMS** includes significant changes to enhance the proactive, strategic, and risk-based approach to security in the aviation industry. Substantial guidance on the supply chain has been updated, focusing on supporting the **External Service Provider concept.**

www.iata.org/sems

IATA

3. International Regulatory Overview

3.1. Aviation Security

- IATA's aviation security strategy is simple:
- Drive improvement in aviation security system performance and response.
- Drive government trust and confidence in the airline Security Management System (SeMS) principles.
- Collaborate on the assessment of evolving threats and deployment of moderate responses.
- Reinforce efficiencies in security practices by adopting risk-based approaches to oversight and measures.
- Support innovation that enables smoother facilitation.

2024 ICAO Milestones

In 2024, we noted the 80th anniversary since the signing of the Chicago Convention and the 50th anniversary of Annex 17–Aviation Security. Congratulations to ICAO for these important milestones.

SeMS Workshop | November 2024

The session saw the attendance of nearly 50 participants from key aviation industry stakeholders from the airline, regulator and security service provider constituencies representing various geographic regions. This third session of the IATA SeMS Workshop series drew robust discussion on the challenges and opportunities for evaluating functional criterion in the benchmarking of SeMS. The event exemplified another opportunity in promoting and facilitating the adoption of SeMS within the aviation industry through collaborative industry engagements between key aviation stakeholders.

Since the inception of the SeMS concept in 2007, SeMS continues to develop, gradually evolving from not only being a mandatory requirement for IATA by virtue of the IATA Operational Safety Audit (IOSA) but also being adopted by other aviation industry stakeholders such as Regulators and Airports.

Meanwhile, the body of IATA SeMS content has continued to evolve now including not just SeMS-related provisions in the IOSA Standards Manual (ISM), but also various guidance materials and SeMS capacity and competency tools. From SeMS training courses, the IATA SeMS Manual, the IATA SeMS Toolkit for External Service Providers (ESPs), to IATA's new SeMS Certification Program, there is now a wide range of resources available for aviation industry partners to utilize in the formulation and implementation of their SeMS strategies.

The aim of the ongoing IATA SeMS Workshops is to support the implementation of the IATA SeMS Strategy in terms of consistency and standardized structure that facilitates effective, efficient, and more uniform security standards throughout the aviation industry. In this third session, the focus was centred on identifying potential functional criterion and key performance indicators (KPIs) for evaluating the effectiveness of functional elements within SeMS.

The objectives of the workshop are summarized as follows:

- Share views and approaches by different aviation industry partners towards two key elements of SeMS: Incident Management and Quality Assurances.
- Discuss and gather potential KPIs and performance measurement criterion for Incident Management and Quality Assurance activities for further discussion & development for future testing.

- Based on the initial KPIs developed and tested, provide recommended SeMS implementation performance measurement criterion to the wider civil aviation industry ecosystem with the appropriate accompanying advocacy actions.

Aircraft Operator Security Program (AOSP) and Supplementary Station Procedures (SSP)

One perfect example of the lack of harmonization and effectiveness in the interpretation and implementation of new Annex 17 provisions by States is the current confusion in the implementation of the new Standards 3.3.1 and 3.3.2 for AOSP and SSP respectively. The need for an AOSP developed by each aircraft operator arose in 1974 with the first edition of Annex 17, and the requirement for all States of the Operators and States of the operations to ensure that all aircraft operators develop AOSPs has been present in Annex 17 for almost four decades in the form of a single standard applicable to all domestic and foreign aircraft operators.

Historically, a few States and IATA outlined administrative challenges with a single standard applicable to all aircraft operators. This was despite a review and approval of AOSPs by States for their domestic operators, they were not recognized by the States of operations for foreign airlines. Owing to the work of the AVSEC Panel, ICAO endorsed with Amendment 18 (2022) two Standards, one for AOSP and the State of the Operator (3.3.1) and a supplementary Standard 3.3.2 for SSP addressing the additional measures that could be necessary for meeting the requirements of the States of the operations when these measures are not already addressed in the original AOSP.

Under the revised Annex 17 provisions, AOSPs are reviewed/approved by the States of the (domestic) Operators, when SSPs, when required, are reviewed/approved by the States where foreign operators conduct their operations.
ICAO developed very clear impact assessments in a State Letter sharing Amendment 18 in March 2022 (and corrigendum in April 2022), then shared initial guidance material (Chapter 15) on their public website in June 2022. But the adoption and comprehension by States has been limited.

IATA held a workshop on AOSP and SSP in June 2024 in Singapore with regulators and airlines from various regions to delve into the current challenges on the implementation of these new provisions and propose solutions. IATA then proposed adjustments for Annex 17 and the ICAO guidance material through the relevant AVSEC Panel Working Groups.

Finally, IATA developed additional guidance material and user friendly tools for airlines and States that are made available in the SeMS Aviation Community (contact aviationsecurity@iata.org for access) and shared publicly in the different IATA Aviation Security websites.

2024 is an ICAO Assembly year and IATA will continue its advocacy for the most successful and effective implementation of both Standards 3.3.1 and 3.3.2 in 2025, with the view of drastically reducing duplicative and unnecessary administrative burdens on aircraft operators.

Hold Baggage Security Procedures

Another example highlighting relevance of international guidance aligned with contemporary operational procedures is implementation of security measures for hold (checked) baggage.

Since 2006, all hold baggage intended to be transported on international flights must be screened at origin. This was a new Standard initially introduced in 2002 with a deferral date "from 1 January 2006", as confirmed with Amendment 11 in 2006. In addition, aircraft operators must only transport hold baggage of persons that have been properly identified as accompanied or unaccompanied, screened to the appropriate standard and accepted for carriage. All baggage should also be recorded as meeting security criteria and tracked during their entire journey for reconciliation purposes with their owner upon arrival.

The very specific Annex 17 requirement for "additional screening" on the baggage of persons that are not on board (the infamous Standard 4.5.3 creating the need for potential baggage offload when its owner is not onboard the same flight) only

existed from 2006 to 2011 as an additional protection in case the screening of all hold baggage at origin was not correctly implemented.

Since 2011 with Amendment 12 to Annex 17, the requirement for "additional" screening was removed. Consequently, from an interpretation point of view, there is no longer any need to offload the hold baggage of a passenger that is not onboard the same flight, provided the hold baggage has been properly identified, and screened to the appropriate standard. All hold baggage is always tracked for operational reconciliation and customer service purposes by the aircraft operators.

In 2021, IATA airlines introduced, in a Recommended Practice contained in the Passenger Service Conference Resolution Manual (PSCRM), the UNAR concept with unaccompanied baggage that could travel ahead of the passenger if all requirements for travel, including security, are met (which aligns with Annex 17 provisions). According to a survey conducted by the IATA Baggage team in the last quarter of 2024, the UNAR concept is implemented in more than 18 States. The concept of synchronic physical reconciliation between hold baggage and its owner ensuring that both are physically present on the same flight is outdated and futile. UNAR fully recognizes the quality of hold baggage screening prior to loading. Whether or not the owner is physically present on the same aircraft is inconsequential given the quality of the implementation of 100% hold baggage screening systems, and the protection of screened baggage in place, that should mitigate any risks.

IATA developed additional guidance material for Hold Baggage Security Procedures that have been shared with relevant Working Groups of the AVSEC Panel for ICAO guidance update purposes, but also for airlines and States. All material and tools are made available in the SeMS Aviation Community (contact aviationsecurity@iata.org for access) and shared publicly in the different IATA Aviation Security websites.

Unfortunately, despite the Annex 17 revisions and introduction of the UNAR concept, some States remain stubbornly resistant and insist on outdated and unnecessary passenger and baggage reconciliation, despite the implementation of screening and protection measures. https://www.iata.org/en/programs/security/

Incident Reporting

The reporting of occurrences and incidents is a long-standing operational posture in the safety environment. The notification and exchange of information on "incidents" was introduced in the ICAO Annex 13 on Aircraft Accident and Incident investigation back in 1973, before Annex 17 on Aviation Security was created in 1974.

IATA has collected data from safety incidents and occurrence reporting for decades, and the extension of the existing safety reporting taxonomies for considering security incidents became evident during the last decade. Safety incidents could be reclassified as security incidents during investigations and many incidents are shared between safety and security depending on their intensity (unruly passenger incidents being a great example).

The need for harmonized security reporting taxonomies for stakeholders, extending to External Service Providers (ESPs) implementing security measures on behalf of airlines under an outsourced business relationship, has been reinforced by new mandates from various authorities seeking more and more reporting of suspicious activities from all entities.

ICAO produced useful guidance material on Incident Reporting and Taxonomy shared publicly, and IATA developed additional guidance material on Incident Reporting that are available in the SeMS Manual (Edition 8), with abstracts made available in the SeMS Aviation Community (contact aviationsecurity@iata.org for access) and shared publicly in the different IATA Aviation Security websites.

3.2. ICAO AVSEC Panel

Amendment 19 to Annex 17

2024 was the year of the 80th anniversary of ICAO, 50th anniversary of Annex 17, and 23rd anniversary of the tragic events of 9/11 which paved the holistic reformation of Annex 17 with Amendment 10 (2002) introducing all contemporary international provisions, followed by Amendment 11 (2006) underpinning the newly created ICAO Universal Security Audit Program (USAP) to measure the Effective Implementation (EI) of Annex 17 Standards in States.

More than 20 years after these important milestones, the global EI of Annex 17 Standards in States as measured by USAP is still not optimal. Moreover, a high number of States are yet to achieve EI of the many core security Standards introduced in 2006. It could be wise to recall the original aims and objectives of ICAO back in 1944, with the creation of the Chicago Convention, in particular the development of principles and techniques to meet, inter alia, the needs for safe (and secure), regular, efficient, and economical air transport. All air transport operators need a safe and secure working environment, but also the effective implementation of a global regulatory framework that ensures regularity, effectiveness, and economical sustainability.

In this context, the continuous improvement and refinement of Annex 17 is crucial for avoiding any misunderstanding and misinterpretations of global security provisions by the States that translate these international provisions into their national legislation and security programmes – which are then imposed on air transport operators. Any gap in the interpretation of global Annex 17 Standards by States could create irregularities, implementation of inefficient measures, in addition to generating additional costs and unnecessary burdens for all industry stakeholders. States and ICAO should be recalled that all airline operators registered in the IATA Operational Safety Audit (IOSA) program must implement IOSA Standards that are fully aligned with current Annex 17 provisions, meaning that aircraft operators are the most impacted by any gaps of interpretation of Annex 17 provisions between the States where they operate.

As the last amendment to Annex 17 has been circulated to States and industry in March 2022, we truly hope that next Amendment 19 could be finalized in 2025 by incorporating all the proposals for improvement and finetuning that have been presented by States and the industry.

These proposals cover clarifications on the need of SSP, clarifications on Incident Reporting, extension of the Recognition of Equivalence concept, and clarification with Hold Baggage requirements. These proposals are essential for improving the regularity, effectiveness, and economic sustainability of air transport operations. States need also to recognize the risk assessments performed by operators and include them in their national programmes for consistency purposes with the current practices and standards in the industry.

3.3. Air Cargo Security

Overview

2024 was a bumper year for global air cargo, with a marked rise in demand, capacity, and yields, underpinned by booming e-commerce and international trade[1]. The global economy depends on air cargo as a facilitator of trade and the provision of essential healthcare products and services. Over 62 million metric tons of air cargo are transported annually, accounting for approximately 35% of world trade by value[2].

The reliance on global air cargo for economic prosperity, and wellbeing brings new security challenges and vulnerabilities. The threat landscape impacting air cargo and supply chains continues to evolve at a rapid pace, exemplified by the July 2024 Improvised Incendiary Device (IID) Act of Unlawful Interference.

[1] Air Cargo Demand up 9.8% in October 2024 - 15th Month of Consecutive Growth

[2] IATA - Cargo

2024 brought renewed attention and focus on air cargo security, cementing the critical need for a safe, secure, and resilient global air cargo and supply chain system.

Improvised Incendiary Device - Act of Unlawful Interference

Arguably the most significant event impacting air cargo security since the 2010 Yemen incident occurred in July 2024. Improvised Incendiary Devices (IID) were concealed and shipped inside parcels in Europe, which subsequently caught fire at a logistics facility and on the tarmac, prior to loading on an aircraft. The incidents caused localised damage but thankfully, no fatalities or damage to aircraft were reported.

The incidents nonetheless highlighted a vulnerability in the air cargo system, since the IIDs were designed to circumvent existing security controls and designed to intentionally cause damage and disruption. In September 2024, a European member state reported the matter to the International Civil Aviation Organization (ICAO) as an Act of Unlawful Interference (AUI).

The IID AUI caused significant disruption to the air cargo sector, with the associated impacts still being felt today. The response, including potential readjustment of compensatory measures remains ongoing. Further details on this IID AUI and the impact on industry can be found in section 5.4 of this report.

In support of our members and industry partners, and in close partnership with our various industry Working Groups, IATA's response to the IID AUI incorporated the following:

- Direct engagement with relevant national regulators to consolidate and highlight specific implementation challenges and encourage appropriate industry pre-decisional consultation and engagement regarding additional security requirements.
- To ensure industry-wide consistency, IATA urgently reviewed the standard messaging framework to accommodate additional data filing requirements required by some governments. The revisions were endorsed and released for industry in October 2024.
- Some governments require airlines to attest a 'business relationship' with supply chain partners (freight forwarders and shippers, including at house level). To assist airlines in implementing these requirements in a consistent and orderly fashion, a template 'Established Business Relationship Statement' was developed by a group of US airlines in conjunction with Airlines for America (A4A) and IATA in September 2024.
- IATA continues to engage our relevant industry governance groups on the implementation effectiveness of the enhanced security requirements imposed by some government and the broader industry-wide response.
- At the international level, IATA will continue our collaboration with international partners, including the International Civil Aviation Organization (ICAO), other trade associations and national governments to encourage and influence a unified and harmonized response.
- In close consultation with the Cargo Security Working Group (CSWG), IATA has drafted new guidance material to assist airlines and other aviation stakeholders with the implementation of appropriate mitigation measures to address the IID threat. The first version of the guidance is expected for release in Quarter 1, 2025.

IATA Cargo Security Working Group

IATA's Cargo Security Working Group (CSWG) is tasked with reviewing all matters related to cargo security to ensure critical coordination between government and industry. The CSWG membership includes Subject Matter Experts from 15 member airlines, supported by Observers. The CSWG aims to ensure cargo security requirements are, wherever practicable, compatible with the interests and constraints of the airline industry and aligned with:

- International aviation security standards, recommended practices, and guidance (e.g. ICAO Annex
- 17-*Security*, ICAO Annex 9-*Facilitation*, and Doc. 8973, Aviation Security Manual);
- National and regional aviation security regulations and amendments.
- IATA Security Management System (SeMS) Manual.
- IATA Operational Safety Audit (IOSA).
- IATA Cargo Border Management Strategy.

In 2024, the CSWG convened two in-person meetings combined with a series of virtual meetings. The CSWG was a significant contributor to IATA's ongoing response to the July 2024 IID AUI, which ultimately dominated the group's focus in 2024.

ICAO Working Group on Air Cargo Security (WGACS)

The IATA Secretariat is a member of the ICAO Aviation Security Panel, Working Group on Air Cargo Security (WGACS). Through active participation and engagement on the WGACS, IATA aims to ensure industry views and priorities are appropriately aligned and considered at the international level. In 2024, IATA's participation in the WGACS was heavily focused on the IID AUI, combined with cargo security related revisions to international aviation security guidance material.

Pre-Loading Advance Cargo Information (PLACI)

In 2024, various States have progressed trials and implementation of PLACI programs. IATA continued to support industry, regulators, and international organizations to ensure PLACI programs are aligned through global standards to achieve the best overall security results whilst minimizing impacts on the air cargo industry. To support the evolution of PLACI, IATA worked throughout 2024 with implementing authorities in Canada, the EU, the United States, and the United Arab Emirates to align their respective mandated requirements with airline industry constraints and expectations. IATA also held a PLACI dedicated workshop in the UAE in May 2024 with 300 delegates from 32 countries and further refined the IATA PLACI standard procedures, resulting in a 6th edition of the PLACI Manual issued in December 2024.

2nd US-EU Air Cargo Security Summit

IATA jointly organized and participated in the 2nd US-EU Air Cargo Security Summit, held in Dublin in November 2024 which included delegates from the Transportation Security Administration (TSA), European Commission, airlines, supply chain partners and trade associations. Key cargo security matters impacting joint United States and European interests were discussed and progressed including the July 2024 IID AUI, National Cargo Security Program Recognition, innovation, and future cargo security strategic priorities.

Consignment Security Declaration Reform

In 2024, IATA continued work on proposed reforms to Resolution 651, Recommended Practice, and associated guidance.

Summary

From a cargo security standpoint, 2024 proved to be a challenging and somewhat disruptive year for the industry. The IID AUI underscored the critical importance of protecting global air cargo and supply chains.

Moving into 2025 and beyond, IATA's cargo security strategy will integrate the following key priorities:

1. Globally harmonised air cargo security measures, enshrined into appropriate international framework.

2. Prioritisation and advocacy for a globally harmonised cargo security regime over the implementation of extraterritorial cargo security measures and programs.

3. Risk-based air cargo security framework, underpinned by appropriate pre-decisional consultation and commensurate to the level of risk.

4. An appropriate balance between robust security outcomes and global air cargo flows.

5. Thorough and coordinated consideration of the evolving threat landscape impacting air cargo and supply chains.

3.4. Regional Security

Europe (including Turkey, Israel, and Russia)

The European Commissions Directorate General Mobility and Transport (DG MOVE) continues to be significant policy interest to IATA as the Commission proactively works to make valued amendments to Implementing Regulation (EU) 2015/1998 and related EU Decision C (2015) 8005. Throughout 2024, IATA participated in the Stakeholders Advisory Group on Aviation Security and the EU Integrated Aviation Security Risk Assessment Group (IRAG) for conflict zones. As well as supporting the US TSA Regional Industry Summits (RIS), working towards Recognition of Equivalence (RoE) of aircraft operator measures as regulated by the EC.

Most notably work continues to resolve issues associated with the COMMISSION IMPLEMENTING REGULATION (EU) 2024/2108 of 29 July 2024 amending Implementing Regulation (EU) 2015/1998 as regards certain urgent aviation security measures regarding equipment for the security screening of liquids, aerosols, and gels.

Asia Pacific

Summary of the IATA India Security-Facilitation Workshop (April 2024):

- The IATA Security-Facilitation Workshop held in New Delhi focused on addressing regulatory and security challenges in India.

- Attended by 100 participants, including representatives from Bureau of Civil Aviation Security (BCAS), Director General – Analytics & Risk Management (DG-ARM), Bureau of Immigration (BOI), and airlines operating in India.

- Provided a platform for collective industry engagement with top government regulators.

- Out of 12 identified challenges, 4 were resolved during the workshop, with the remaining 8 set for further review by BCAS and other authorities.

- Regulators, particularly BCAS leadership, actively engaged and addressed immediate issues, demonstrating a willingness to collaborate.

- Following the engagement of the workshop, BCAS issued a Corrigendum in September 2024 to expand the pool of authorized security service providers, addressing a critical manpower constraint raised during the workshop.

Americas

Progress on several key security priorities throughout 2024, mainly focused on efforts in relation to RoE and One Stop Security (OSS) and TSA engagement.

Continued advocacy for OSS implementation in coordination with ICAO and States, despite challenges raised by the TSA. The group sees this as a long-term objective and will persist in lobbying stakeholders for broader acceptance.

Continued representation via the TSA Aviation Security Advisory Committee (ASAC). Several

recommendations were made and currently under TSA Administrator consideration.

North Asia

In 2024, the IATA Beijing office continued to maintain active communications with local industry stakeholders such as the Civil Aviation Administration in China (CAAC), airlines, airports, and academic institutions, on aviation security topics.

- A regular meeting scheme has been established between IATA and CAAC to address the concerns of member airlines, exchange progress and explore potential cooperation opportunities.
- With the support of central security team, two regional security workshops were held in the region to raise local airlines' awareness of IATA security developments, promote security related activities, and facilitate in-depth discussions and experience sharing on topics of mutual interest.
- Discussed and gathered common security needs of airlines through regional workshops and individual meetings with local members, including threat assessment and cybersecurity training, sharing of external service provider (ESP) management practices at overseas stations, open-source security information, etc. Based on these needs, IATA Beijing office will further assist the central security team in 2025 to engage more deeply with local stakeholders.

3.5. ICAO Security Week & Muscat Declaration on Aviation Security & Aviation Cybersecurity

IATA attended ICAO's annual security week event and was provided an opportunity to lead a panel intervention.

Safety and Security as Top Priorities:

- Aviation security remains foundational to IATA, ICAO, and the industry, underscoring the importance of maintaining trust in systems and principles amidst challenges.
- Risk-Based, Outcome-Focused Policies - emphasize innovative frameworks like management systems and adaptable oversight.
- Information Sharing – a call to commit to timely incident and cybersecurity information sharing to build resilience and enhance risk assessments.

Muscat Declaration was officially adopted on the 11 December 2024, during the Ministerial Segment of ICAO Security Week 2024.

This pivotal document underscores the collective commitment of ICAO Member States and global stakeholders to advance aviation security and resilience, ensuring the implementation of strategies that protect passengers, infrastructure, and operations worldwide.

4. IATA Governance Groups and Work Plans Overview

4.1. Security Advisory Council (SAC)

The SAC met twice throughout 2024 in Miami and Geneva, starting with a TSA leadership brief focused on issues such as oversized LAGs, OSS arrangements, and technology certification discrepancies between the US and ECAC. SAC members emphasized the need for tangible progress on risk assessment processes and improvements in aviation security frameworks.

Additionally, the SAC covered the following throughout 2024:

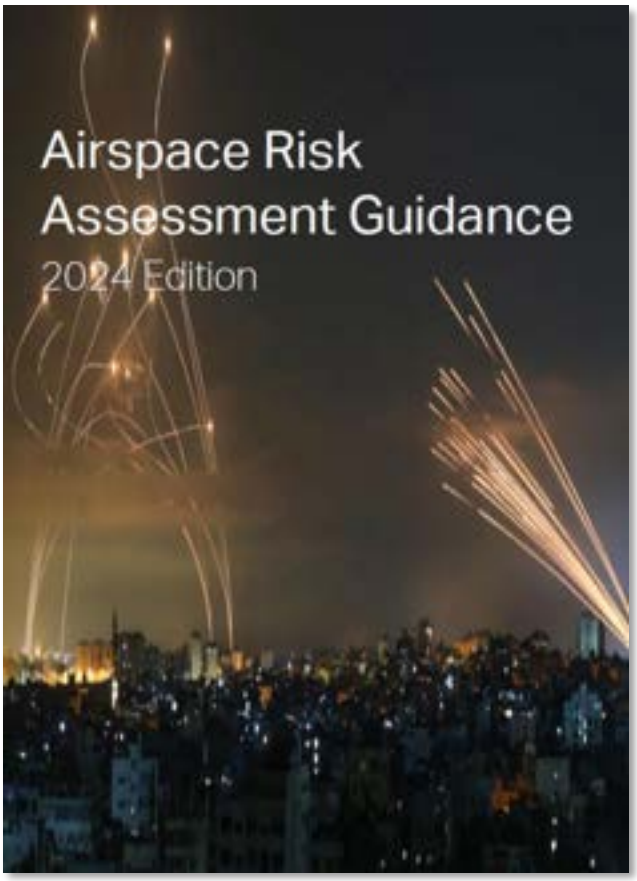
- Strategies to improve international OSS coordination. The SAC continues to support OSS adoption.
- Endorsed a workshop for the Aviation Security Trust Framework (ASTF) and addressed challenges in AOSP/SSP implementation.
- SAC-endorsed workshop in India in April 2024, focused on security and facilitation, and a comprehensive review of passenger security efforts,
- SAC reviewed a geostrategic risk framework focusing on strengthening risk assessments and NOTAM reform related to conflict zones.
- SAC supported SeMS Certification process and KPI adoption, with strong support for security incident reporting and industry engagement.
- SAC noted an increasing concern around fraud and organized criminality in aviation was highlighted, with IATA set to map an internal approach to fraud risk management.
- SAC supported the IATA SeMS Workshop in November 2024 and collaborative discussions with regional security groups.
- SAC supported IATA's advocacy strategy pertaining to the July 2024 IID AUI.
- Continues to address evolving security challenges, with a focus on outcomes-driven regulatory compliance, industry engagement, and the strategic alignment of international security frameworks. Moving forward, IATA and SAC will prioritize strengthening partnerships, improving communication strategies, and addressing ongoing global security risks.

4.2. Geopolitical Risk Task Force (GRTF)

Geopolitical risk and ongoing conflicts that have negatively impacted the availability of global civil airspace which will almost certainly remain a major source of disruption and volatility for the aviation sector in 2025. These include the conflict between Ukraine and Russia, the conflicts between Israel and Hamas in Gaza, and the possible expansion of conflict into adjacent areas, as well as other locations subject to geopolitical tensions. Our strategic partners assess that there is a worsening security and stability outlook for 2025, with only minimal improvements. For most countries, the overall stability trajectory will mean a continuation of volatility.

The GRTF are focusing on best practices. The GRTF met twice in 2023 and once in 2024. The GRTF has identified several objectives since it was established. Each of these requires collaboration with both internal and external organizations, as well as the input received from IATA task force members.

Issue	Description
Risk assessment methodologies	Airspace risk assessment guidance document as published and hosted on MS Teams.
As per page 12 of 38, of the Safe Skies Forum Report 2023, Maintaining Safe Airspace - Managing Information	NOTAM reform (security). GRTF to develop arguments for why the use of NOTAMS for conflict zones is or is not fit for purpose in terms of flight dispatch planning.
Industry to Government Baseline Call	Multilateral, open-source medium to near term information sharing platform between airlines and governments.
GNSS related interference	GRTF to assess from a security/direct intentional perspective.
IATA FAA Liaison Desk and ITOP	GRTF to provide IATA guidance on scoping a 24/7 capability in prevention/reactive to conflict zone effected airspace



4.3. IOSA SEC Task Force (SEC TF)

The Security Task Force (SEC TF) of the IATA Operational Safety Audit (IOSA) Program functionally reports to the IOSA Oversight Group for IOSA activities and secondly to the Security Advisory Council (SAC) in support of the development of security policies, position papers, or other security-related activities or projects.

The primary responsibilities of the SEC TF are to ensure continuous update and improvement of the IOSA Standards and Recommended Practices (ISARPs) that are contained in the IOSA Standards Manual (ISM). ISM is applicable to all IOSA-registered airlines and aligned with ICAO Annex 17 (and other Annexes) for its security components.

The SEC TF is also responsible for the ongoing interpretation of the security-related ISARPs that are in different sections of the ISM, aid the IOSA Security Auditors when questions arise, and continuously finetune the related ISARPs guidance material for better interpretation, fostering

harmonized and efficient implementation by IOSA-registered airlines and their External Service Providers (ESPs). ESPs currently implement most of the Operator's security operational functions under outsourcing business agreements, which reinforce the need for strong oversight, coordination, and alignment.

The SeMS concept has been extended to ESPs in the ISM/17 applicable in January 2025, and IATA developed extensive of guidance, tools, and programs for ensuring wider adoption of SeMS among all industry stakeholders with the goal of reinforcing the overall SeMS posture of IOSA-registered airlines and their business partners.

In 2024, the SEC TF worked on the 18th edition of the ISM (ISM/18) and focused on the review and potential adjustment of the security related ISARPs (and guidance material) located in three Sections, namely Ground Handling, Cargo, and Security, where most of the current outsourcing takes place. The objective is to bolster and clarify the narrative on three topics, namely AOSP/SSP, incident reporting and cross-functions and responsibilities between Operators and their ESPs.

ISM/18 will be applicable in January 2026, leaving time for internal awareness and training campaigns (for the IOSA Security Auditors) and wider advocacy activities for promoting the ever-growing SeMS posture of IOSA-registered airlines and their business partners, in particular the ESPs that will adopt SeMS principles via the documents, guidance and SeMS toolkit for ESPs shared in the SeMS Aviation Community (please contact aviationsecurity@iata.org for access), and more importantly demonstrate their SeMS robustness via the new IATA SeMS Certification Program.

As the current SEC TF membership runs until April 2026, SEC TF members will be in a position to further polish ISM standards and related guidance material during the 19th Edition cycle which will commence in 2025. ISM/19 will be applicable in January 2027, meaning 20 years after the introduction of SeMS in ISM in 2007 (ISM/2).

In the context of the 20th anniversary of SeMS in ISM, ISM/19 will focus on the review and adjustments of all ISARPs directly linked to the SeMS key elements that are shared and interlinked between Operators and their ESPs. These shared SeMS key elements are Incident Management (including incident reporting and rectification actions), Oversight Functions (internal and external quality control and quality assurance) and Threat Assessment and Risk Management (at both Operators and ESPs levels).

5. Key Perspectives

5.1. Opinion Piece on Hold Baggage Security Reform

Operational Challenges with Baggage Reconciliation

Airlines face significant delays and operational inefficiencies owing non-reformed baggage reconciliation requirements akin with evolving international standards and technology. The regulatory protocols, initially implemented for protective security outcomes, now negatively impacts operational efficiency and facilitation, causing missed connections and increased costs.

Historical Context of Baggage Security

Baggage reconciliation emerged as a response to aviation security threats in the 1980s and has evolved with international requirements, including the 100% hold baggage screening mandate introduced in 2006. Despite advances, some of these procedures have become mostly redundant due to improved security technologies and oversight methodologies.

As explained in the Hold Baggage Security Procedures section (in paragraph 3.1), the outdated synchronic reconciliation procedures could be challenged on their security relevance in 2024.

Many jurisdictions have invested in appropriately certificated screening technology and have adequate oversight of controls in place. Thus, the security arguments for reconciliation of passengers and their hold baggage on the same flight is no longer valid.

Request for Regulatory Flexibility

Airlines are seeking adjustments to outdated regulations, advocating for a risk-based approach that would allow for more operational flexibility. This includes leveraging modern screening methods and existing international agreements, like One Stop Security (OSS), to streamline processes without compromising safety or security.

Requiring airlines to track a passenger's exact location within the sterile area during baggage offloading, as highlighted by one airline in their 2024 regulatory discussions, offers no meaningful contribution to protective security.

Security verses Operational Considerations

We emphasize the need to differentiate between security and operational aspects of hold baggage screening. While security requirements remain robust, certain operational processes, like the presence of a passenger on the same flight as their baggage, could be adjusted for efficiency purposes without increasing security risks.

Benefits of Updating Requirements

Implementing more flexible baggage reconciliation practices would reduce operational delays, improve efficiency at airports, and enhance the passenger experience. By focusing on advanced screening technologies and international cooperation, airlines can maintain safety and security standards while minimizing disruptions.

5.2. The Sustainability of Aviation Training

As the aviation industry continues to grow, with passenger numbers expected to reach 5.2 billion by 2025 as per IATA's predictions as issued on 10th Dec 2024, the demand for skilled professionals is higher than ever. The need for effective and affordable training becomes more critical, making the sustainability of aviation training a pressing issue that demands attention.

Many factors affect this sustainability, including the quality of offered training in terms of content, design and delivery, industry needs, in addition to the incurred cost. These factors are interrelated, affecting the security outcome.

In terms of training content, this is highly connected with industry needs, regulatory requirements, and an evolving threat landscape. Identifying key competencies, complying with evolving regulations, and focusing on human factors are essential. There is no value in running training programmes which have outdated content

and are no longer required by the industry. Just as the threat landscape for aviation is proving to be dynamic, the simple correlation that training programmes need to be reviewed and updated. It may seem time and effort intensive, but this is an essential action required to maintain currency and effectiveness.

Designing a training programme is no small feat. Extreme care must be taken to consider the target audience, delivery method and impact. The importance of considering human factors, cognitive and language capabilities in addition to the cultural differences to be able to achieve the required outcome of such training cannot be understated. Without being overly bureaucratic, oversight activities to confirm the quality of these training programmes must be applied, especially as there have been reports of training providers having abused the system and passing failed trainees.

Owing to civil aviation being the most regulated transportation mode; aviation training is heavily driven by compliance with stringent regulatory standards. This is addressed by designing technical training which is specialised and practical, focusing on specific skills and certifications needed for roles. While this ensures safety and efficiency, it can also stifle critical thinking, which is usually offered by higher education.

To address this, training programmes must incorporate:

- Scenario-based learning,
- Problem-solving exercises and reflective practices.
- Encouraging trainees to question assumptions, and.
- Exploration of different perspectives can enhance their ability to navigate complex environments.

Keeping in mind the clear distinction between technical training and higher education in aviation, the latter provides a broader understanding of aviation, preparing individuals for a wider range of career opportunities, including leadership and research positions, which are becoming increasingly sought after.

Furthermore, and in terms of delivery, the industry faces the challenge of integrating new technologies and methodologies to keep up with evolving threats and operational demands.

Virtual Reality (VR) and gamification are emerging as innovative solutions, offering immersive and engaging training experiences. These technologies can simulate dangerous scenarios, helping trainees develop critical decision-making skills in a safe environment.

Artificial Intelligence (AI) is revolutionising aviation security training. AI-powered simulations and predictive analytics help create realistic training scenarios and identify emerging threats. Bespoke training programmes tailored to specific needs ensure that security personnel receive targeted and effective training. With that said, attention must be paid to the accessibility to these technologies from an affordability viewpoint.

Training has always been expensive, but the current economic climate exacerbates this issue. Organisations, even large ones, often view training as a cost rather than an investment, leading to budget cuts that impact the quality and availability of training programmes. This trend is concerning, especially when the industry faces operational challenges to face the dynamic threat landscape that requires upskilling current staff and training new professionals.

The future of aviation training lies in balancing compliance, innovation, and cost. By integrating new technologies, fostering critical thinking, and aligning training with industry needs, the aviation sector can ensure that its workforce is well-prepared to meet the challenges of a rapidly evolving landscape. The sustainability of aviation training hinges on ensuring that training is both accessible and effective.

By Rania Khbais, MSc AFHEA ARAeS

Senior Lecturer in Aviation Security

Buckinghamshire New University

5.3. 20 Years of ICAO and Concordia Aviation Security Professional Managers Course (AVSEC PMC)

In 2004, the International Civil Aviation Organization (ICAO), in collaboration with the John Molson School of Business (JMSB) at Concordia University, Montreal, Canada, launched the innovative Aviation Security Professional Management Course, (AVSEC PMC), with the original aim of providing aviation security middle and senior management personnel with new management skills and a greater understanding of the application of Annex 17 provisions, while maintaining a creative and pedagogic philosophy as stated on the ICAO webpage.

Back in 2003, with significant change imposed by the aftermath of 9/11, a totally new Annex 17, and a new ICAO USAP programme, the ICAO Security Section and JMSB created a totally new training product that was the most advanced aviation security training programme and official certification in existence. We now have the Master of Science (MSc) in Aviation Security offered by ICAO and Buckinghamshire New University, in the UK, but the AVSEC PMC remains the first of its kind globally.

In 2003, the need to uplift security personnel expertise to create new "security managers" capable of managing security systems in the most creative, versatile, and effective manner was clear, hence the course architects created a three-month hybrid course with two face-to-face sessions of one week, combined with 10 weeks of intense e-learning sessions between the two face-to-face sessions. As with any advanced academic course, the rate of success was never designed to be at 100%. The course integrated significant challenges designed to emulate the professional security manager's real working environment including the intensity of the work required, the international outlook of the course, and variety of professional origins of the participants, that were essential for creating totally new working conditions and challenges for all participants.

The first AVSEC PMC course was launched in Casablanca in July 2004, more than 20 years ago, with participants that are still working and performing in the current aviation security eco-system today.

In 2005, the AVSEC PMC was translated and delivered in French language, making the AVSEC PMC the first ever multi-lingual, hybrid e-learning aviation security course designed to create a family of new aviation security managers capable of maintaining contact via the AVSEC PMC hybrid community, which is still active today.

The statistics for 20 years of AVSEC PMC are considerable with more than 1200 alumni or successful graduates from all the regions of the world. The list of ICAO AVSEC Professional Managers is published on the ICAO website, and it could be worth checking whether your current colleagues have graduated the course.

IATA is proud to continue its support for the ICAO/Concordia AVSEC PMC, and celebrate the 20th anniversary in its English format.

The AVSEC PMC, in 2004, opened the path for the introduction of the Security Management System (SeMS) concept in the IOSA Standards Manual (ISM) in 2007, and then SeMS guidance in the ICAO Aviation Security Manual (Doc 8973, Restricted) in 2010.

The SeMS journey continued with the IATA SeMS Manual launched in 2017, then the creation of an holistic SeMS Aviation Community (contact aviationsecurity@iata.org for access) in 2022. The SeMS Aviation Community developed, in May 2024, the first SeMS Toolkit designed for External Service Providers (ESPs) which is freely available in the SeMS Aviation Community.

Finally, the SeMS culmination could be achieved with the new IATA SeMS Certification Program launched in October 2024 (Press release).

IATA will also be proud to celebrate the 20th anniversary of the AVSEC PMC in its French format in 2025.

5.4. IID AUI Analysis

An analysis of the July 2024 cargo Act of Unlawful Interference: Industry challenges and lessons learned.

In July 2024, several shipments containing unstable incendiary devices, known as Improvised Incendiary Devices (IIDs), were allegedly sent via air cargo in Europe. The IIDs were reportedly sent inside parcels and consisted of electrical items and flammable liquids that caught fire on the apron during transfer to an aircraft and inside a logistics facility. In September 2024, a European Member State reported the incident to ICAO as an Act of Unlawful Interference (AUI). Suspects are in custody and facing legal proceedings in Poland.

The reasons behind the interference remain unknown as investigations continue. However, the actions taken by regulatory authorities clearly suggest that these incidents were deliberately aimed at causing damage and disruption.

The ongoing response to these events warrants several points of discussion and potential lessons learned.

Evolving Threats to Air Cargo Security and Uncoordinated Responses

Firstly, these events clearly underscore the evolving threats to air cargo and supply chains, highlighting the critical need for enhanced compensatory measures to mitigate associated risks. Several States responded by imposing additional security requirements on cargo destined for their territories. Unfortunately, these measures were not appropriately planned, developed, and coordinated which created significant complications, confusion, and implementation delays. But rhetorically, are they ever? We operate in a regulated system of known measures purposed for known threats and risks, yet the dynamic nature of these threats often outpaces our responses.

The unconventional and unprecedented nature of the AUI justified an immediate and emergency response. In such scenarios, it is understandable that temporary measures may be implemented that exceed existing international standards. Over the last two decades, coordinated efforts have been made to develop, revise, and enhance international cargo security standards that have incrementally improved security without compromising facilitation.

Nonetheless, some additional measures imposed by certain States in response to the AUI circumvented and disregarded existing international standards. In some cases, the additional measures inadvertently reverted to a lower standard, ignoring recent internationally agreed efforts to enhance such standards. Furthermore, the decoupling from international standards precipitated a fragmented, extraterritorial approach, undermining combined security efforts and disrupting global trade and cargo flows.

The air cargo sector is inherently diverse and complex, with distinct operational differences across various supply chain and air carrier models. Some of the additional security measures failed to account for these vast operational differences and assumed a 'one-size-fits-all' approach. Industry was not appropriately consulted and engaged in the planning and development phase resulting in the imposition of disjointed and unsuitable measures, some of which were subsequently repealed, reviewed, and replaced.

Moreover, some additional requirements were based on the respective jurisdiction's domestic regulatory frameworks and terminology that did not align with existing international standards, leading to misunderstanding in a global context.

Limitations in Information Sharing and its Impact on Risk Management

The unprecedented nature of this AUI also demonstrated the limitations of information sharing. It is not always possible to share or receive the threat information we desire or expect. In this case, segments of industry were left with *no* tangible background or information pertaining to this recent AUI. As a result, they were forced to rely upon patchy, often inaccurate media reports. This lack of official information made effective risk assessment nearly impossible, constraining industry's ability to understand and respond to the threat.

Need for a Flexible, Coordinated, and Standards-Aligned Approach

Acknowledging the limitations of information sharing, it is crucial to establish a balance between State level information and the fundamental principles of information sharing and international cooperation enshrined in Annex 17-*Security.* While States must protect security sensitive information (or intelligence), this should not impede the obligation to share sanitized, factual, relevant information. Industry and government alike require timely, baseline information surrounding the nature of threats impacting their operation/jurisdiction to *proactively* respond with appropriate mitigation strategies. Otherwise, the associated risks are merely shifted rather than effectively mitigated at the international level. The recent cargo AUI highlighted significant gaps and markedly absent international cooperation and information sharing, which only prolonged vulnerabilities and delayed a cohesive global response.

Conclusion

The ongoing response to the cargo AUI revealed several challenges, but more importantly, it presents opportunities for improvement. We need to engender a flexible, adaptable, and resilient air cargo system that can respond to emerging threats in a coordinated manner. Regulatory controls should be commensurate, risk-based, and developed in appropriate consultation with industry through pre-decisional engagement. Finally, international standards should be appropriately considered during the development and implementation phase, with any revisions sufficiently coordinated at the international level to ensure consistency and harmonization.

Due regard for these principles will ensure emerging threats are addressed in a swift, coordinated, and organized manner, to the benefit of governments and industry alike.

5.5. Addressing the Gap in Non-Punitive International Reporting Structures for Aviation Security

Threats to one organisation or region can cascade across borders, underscoring the necessity of collective responsibility and shared solutions. While individual organisations and Civil Aviation Authorities (CAAs) may offer reporting mechanisms, organisational or cultural barriers, such as fear of retaliation or lack of trust in the system, often undermine these. This dynamic reflects the principles of Social Contract Theory, wherein mutual trust between individuals and institutions forms the foundation for cooperation. Without this trust, aviation security systems risk becoming superficial, failing to address the vulnerabilities they aim to mitigate.

At its core, adopting a Security Management Systems (SeMS) approach in a highly regulated sector such as civil aviation emphasises a culture of accountability and continuous improvement. It achieves this through non-punitive occurrence reporting, like the just culture under the Safety Management Systems policy. Thus, the systems approach encourages personnel to report security vulnerabilities or occurrences without fear of doing something wrong.

While the theory is clear, a recent conversation with a participant in one of my AVSEC training courses revealed an opportunity to think this through further. Would an internationally recognised anonymous aviation security occurrence reporting be of interest to the community? It would eliminate the potential for personal blowback by reporting a gap or occurrence in the system that would need to be reported to civil aviation authorities and/or operators all the same.

The participant, employed by a globally recognised aviation organisation, identified areas of vulnerability in their operational environment that the course itself revealed and expressed apprehension about reporting these vulnerabilities. They feared retribution from their employer and, by extension, consequences from the broader regulatory environment, including entities such as

the National Civil Aviation Authority (CAA) or the Ministry of Interior (MOI),

While some national and supranational mechanisms for reporting all types of occurrences may exist, there is seemingly no universally accessible or internationally governed structure in place for a concerned AVSEC professional to report occurrences or apparent vulnerabilities in a way that permits the real issues at hand to be assessed.

It is important to clarify that such a mechanism differs from safety reporting, particularly under adversarial or inquisitorial legal systems. In adversarial systems, security reports often constitute prima facie evidence toward a possible criminal investigation or prosecution, which may, in some jurisdictions, naturally deter professionals from reporting due to fear of legal repercussions.

In inquisitorial legal systems, individuals may be compelled to provide evidence or face criminal charges for withholding information, as demonstrated by the ongoing challenges in South Korea, where authorities have formed the belief that personnel have information. The mix of legal systems complicates security reporting and will likely continue to discourage personnel from coming forward and reporting meaningful gaps.

The real question is: to whom can such concerns be safely reported in operating environments where reporting gaps are inherently discouraged?

While the reporting culture can face challenges, such as concerns about damaging professional relationships or cultural dynamics like 'wasta' (favouritism), it is crucial to recognise that reporting inherently reflects a desire for improvement. Professionals who raise concerns are committed to improving systems, and fostering this mindset is key to enhancing aviation security measures from the ground up. This example underscores how cultural and systemic barriers, such as favouritism or fear of deportation, while varying from region to region, collectively reflect a broader challenge: the suppression of a reporting culture due to entrenched organisational dynamics. Though systems and processes differ between airports and countries, a diversity we celebrate, our collective mission is continually improving, recognising that safe occurrence reporting is our greatest potential to stay ahead of evolving threats. For employees in similar environments, particularly those in vulnerable positions or dependent on their employment status, such a culture creates systemic barriers that discourage reporting altogether. These realities underscore the critical need for an international mechanism that ensures confidentiality, protects reporters, and fosters a culture of accountability, regardless of the local context.

The Case for an International Non-Punitive Reporting System

An international reporting structure, operating independently of individual organisations and governments, could:

- **Encourage Transparency** – Provide a safe channel for individuals to report concerns without fear of professional or personal consequences.
- **Enhance Risk Identification** – Aggregate data from diverse sources to identify systemic vulnerabilities that might otherwise go unnoticed.
- **Foster Trust** – Build confidence among aviation personnel that their concerns will be addressed impartially and confidentially.
- **Promote Accountability** – Hold organisations and regulatory bodies to higher standards by addressing issues that may be overlooked or ignored locally.

Challenges and Considerations

While the concept of an international non-punitive reporting system is compelling, its implementation would require careful consideration of several factors:

- **Governance and Collaboration** – An international reporting system must be overseen by a credible body such as ICAO, IATA, or a new independent entity, with buy-in from airlines, airports, regulators, and stakeholders.

- **Legal Protections** – Ensuring whistleblowers are shielded from retaliation under international law, particularly in weak local protections.

- **Data Security** – Safeguarding the confidentiality of reports while enabling effective investigation and resolution.

Next Steps

To address this gap, the aviation security community must engage in a concerted dialogue:

- **Industry Advocacy** – Encourage key players such as IATA and ICAO to prioritise the development of an international non-punitive reporting system.

- **Stakeholder Engagement** – Convene working groups of industry representatives, regulators, and legal experts to design a framework that balances accessibility, accountability, and confidentiality.

- **Pilot Programs** – Test the concept in a specific region or sector to refine its operations and demonstrate its value.

This issue underscores a critical need: aviation security cannot thrive without a culture of openness and trust. While SeMS provides a foundation, the absence of a truly international, non-punitive reporting structure represents a vulnerability. Addressing this gap is not only a moral imperative but also a strategic necessity for safeguarding the integrity of global aviation security. The aviation community must prioritise this initiative by committing resources, establishing pilot programs, and integrating lessons from safety reporting systems. Only by doing so can we move toward a safer and more transparent future.

By Ben Griffin
IATA AVSEC Instructor

6. Security Management System (SeMS)

6.1. Strengthening Aviation Security Oversight—Adapting to New Realities with SeMS

Civil aviation regulators face challenges in conducting efficient and meaningful oversight of security measures and controls. Their role is essential for ensuring national and international standards are upheld to protect passengers, crew, and aircraft from acts of unlawful interference. However, as new threats emerge and operational complexities grow, traditional oversight methods of creating the rule and inspect are becoming increasingly strained.

To address these challenges, the SeMS approach, coupled with a supporting Aviation Security Trust Framework (ASTF), adopting the use of Verifiable Credentials (VC) for security program information, regulators have a real-world opportunity to optimize their methods and frequency of oversight.

- **Evolving Threats Require New Approaches** – Traditional methods of oversight, like periodic audits, are increasingly challenged by evolving threats such as cybersecurity and foreign interference. Regulators need a shift from rule-based compliance to a risk-based, adaptive mindset to effectively address these new risks.

- **Balancing Security with Efficiency** – Regulators must find a balance between ensuring robust security measures and maintaining operational efficiency. Given the complexity of security measures being implemented by various entities and different jurisdictions, regulators must ensure that measures remain relevant and do not overlap.

- **Resource Constraints Challenge Oversight** – Regulators face limitations in staff and funding, making it difficult to plan allocate resources to the rule-based activities.

- **Self-Assurance and SeMS as Proactive Solutions** – The self-assurance approach, supported by SeMS, allows operators to identify and address vulnerabilities independently, promoting continuous improvement. This approach empowers operators to manage risks and enhances the overall security culture.

- **Enhancing Oversight with Digital Trust Frameworks** – Integrating digital tools like aviation security trust frameworks and verifiable credentials can streamline oversight. These tools enable secure data exchange and allow regulators to focus on developing risk-based oversight approaches from their home base thus reducing time, resource, travel, and administrative constraints.

The Way Forward

The most effective approach to aviation security is often a balance between **self-assurance** and **regulatory oversight**, where each complements the other through mutual reinforcement.

Self-assurance allows operators to take ownership of their security processes and adapt quickly to changing conditions. Government oversight provides a consistent standard and ensures accountability, creating a safety net that catches any gaps or lapses in industry-led efforts.

SeMS enables operators to conduct thorough self-assessments and continuous monitoring of their security practices. Regulators can then focus on validating these processes, using the data and reports generated by SeMS to target their audits and inspections more effectively.

By embracing SeMS, aviation security trust frameworks, and verifiable credentials, regulators can transform their approach to oversight—becoming more adaptable, data-driven, and proactive. This will not only help them keep up with emerging threats but also strengthen a culture of resilience and trust.

7. Aviation Security Trust Framework

On November 18, 2022, ICAO Annex 17 Standards mandated airlines to implement Aircraft Operator Security Programs (AOSP) and where applicable, Supplementary Station Procedures (SSP). These measures align with National Civil Aviation Security Programs (NCASPs), reinforcing the need for robust, unified security frameworks across domestic and international operations. To enable this IATA has conceptually developed a real-world service for regulators and airlines to adopt leveraging emerging verifiable credentials (VC) approaches.

Regulatory Advancements – Airlines are required to align AOSPs with home country standards while addressing unique security requirements in foreign operational territories. This dual-layered regulatory requirement underscores the growing complexity of aviation security management and compliance oversight.

Digital Transformation Imperative – Aviation stakeholders must transition from traditional, paper-based systems to secure, digital frameworks to protect critical documents and exchanges to create tangible levels of trust.

Emerging Digital Standards – Modern cryptographic technologies, including Verifiable Credentials (VC) and Decentralized Identifiers (DID), present promising solutions. These global standards, endorsed by entities such as the World Wide Web Consortium (W3C) and the UN/CEFACT, are being adopted for critical applications worldwide, including digital identity wallets and secure trade documentation.

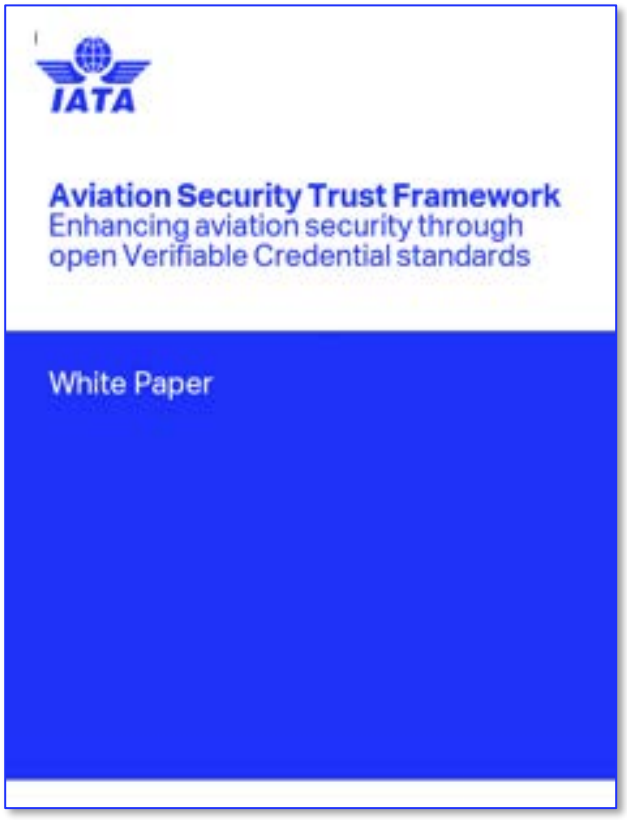
Collaboration in a Digitized World – Building on its history of fostering trust and standardization, the aviation industry is well-positioned to extend this collaboration into the digital domain. IATA is envisioned as a key enabler, bridging physical and digital trust across stakeholders and jurisdictions.

A Framework for Trusted Interactions – By leveraging emerging identity standards, cryptographic technologies, and the collaborative foundation of stakeholders, the proposed framework enables secure, interoperable sharing of critical security documents (NCASP, AOSP, SSP). This ensures document authenticity, integrity, and traceability, addressing global regulatory requirements efficiently and securely.

IATA is poised to lead this transformation by enabling interoperability and trust among aviation stakeholders. The ultimate objective is seamless exchange and recognition of security programs across all jurisdictions, streamlining compliance while enhancing operational security and efficiency.

This executive framework underscores the urgent need for modernized, digitally secure solutions that align with regulatory imperatives and support the aviation industry's commitment to safety, security, and global collaboration.

Please learn more here www.astf.iata.org



8. Products, Training, and Consultancy

8.1. SeMS Manual

IATA released its 8th version of the IATA SeMS Manual in 2024. Major changes included:

Evolving Security Approaches

Emphasis on proactive, strategic, and risk-based security approaches in aviation, with updated guidance supporting the integration of External Service Providers (ESPs) into security frameworks.

Enhanced Documentation Practices:

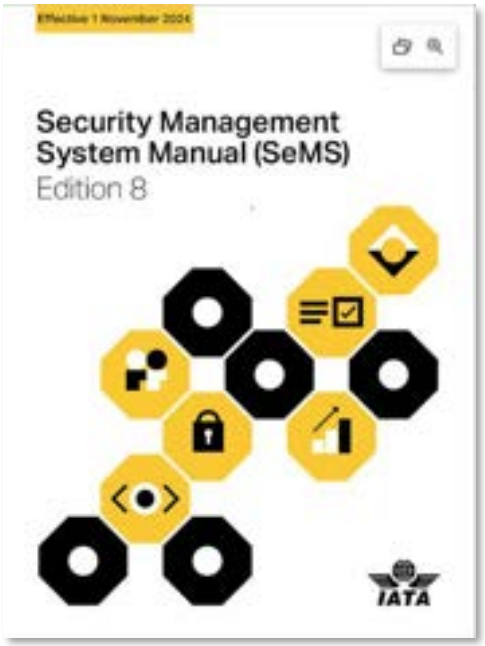
Restructured guidance on maintaining centralized, clear, and consistent documentation tailored to organizational performance and regulatory needs, with a focus on standardization across the organization.

Improved Risk and Incident Management

Updates to risk assessment methodologies, integrating security with safety and cybersecurity operations, and enhanced reporting mechanisms detailing interdependencies among Airlines, ESPs, and Authorities.

New Tools and Resources for SeMS:

Introduction of tools like the SeMS Dashboard Toolkit and Implementation Plan, enabling organizations and ESPs to monitor progress, perform maturity assessments, and ensure compliance with stakeholder requirements. A digital resource includes 150+ questions for deeper SeMS evaluations.



8.2. IATA Training

The IATA Training institute and its 350+ courses and 40+ diplomas is developed around IATA's areas of expertise and commitment to promoting industry standards worldwide. Our training helps businesses operate safely, efficiently, and sustainably, building career opportunities for the people they employ. Through the various industry segments, IATA Training provides respective training programs.

In the area of Aviation Security, with 25+ course titles and 3 diploma programs, the IATA Training Institute's mission is to provide the right competence to the right people, in the right format. The security training portfolio targets a wide audience, whether it is an airline, airport, civil aviation authority or AVSEC service provider, our principal goal is to pass on the crucial understanding about current threats and risks to security and how to manage them together with relevant legal frameworks and regulations.

- Our security courses provide timely information on legislation and strategies for addressing today's security challenges.
- With courses ranging from operations to planning to management, our participants can find training for every step of their career.

- The full catalogue of the security training portfolio can be found at: IATA - Security courses.

2024 IATA Training Review

2024 saw a return to pre-pandemic training capacity. Many organizations have resumed their security training plans and this was reflected by the higher demand for face-to-face classroom training, both at the IATA Training Centres and onsite delivery for clients upon request.

IATA has delivered close to 100 security courses, with a balance of 75% face to face and 25% virtual training.

With a growing number of participants in 2024 and with 800+ students, representing 180+ organizations, IATA Security Training has expanded its audience into more sectors in the aviation industry such as airports, civil aviation authorities, aviation service providers and others.

Training locations include our main training centres in Geneva, Singapore, Montreal, and Miami together with our smaller centres such as Amsterdam, London, Abu Dhabi, and Milan.

In 2024, IATA Training launched a new training venue at its offices in Abu Dhabi, UAE. This modern and new training venue will host courses all year long, from various subject areas enabling industry personnel across the region and beyond to participate IATA Training courses.

Course offered to the public in training centres or virtual classrooms make up 80% of our trainings, with the remaining 20% delivered directly to clients as in house training (in-company).

The five top titles that were in demand by order of attendance:

- Aviation Cyber Security
- Security Management System
- Security Audit and Quality Control
- Aviation Security Management
- Aviation Security Train the Trainer

In 2024, a new course - IATA Airspace Security & Risk Assessment was developed and delivered.

Given the renewed attention and focus on airspace security and geopolitical conflict, this course has already gained significant momentum. IATA expects to add additional courses to the 2025 schedule to meet demand.

IATA - Aviation Cyber Security Management Diploma

The area of cyber security continues to be of high interest, and we see more participants aiming for the new diploma, Aviation Cyber Security Management, which creates high intertest in the industry attracting customers to this unique proposition.

8.3. SeMS Certification

In 2024, IATA released a new certification program on SeMS.

IATA issued a press release on the launch of the SeMS Certification Program representing new levels of investment and partnership into this business asset – CLICK HERE.

9. Annex | Strategic Partners

9.1. Conflict: A Major Source of Uncertainty for Aviation – Dragonfly

Conflicts and geopolitical events will continue to shape decision-making in the aviation sector in the coming years. In 2024, conflict in the Middle East elevated overflight risks there and led to recurrent airspace closures in Israel, Iran, Iraq, Jordan, and Lebanon, among others. This prompted airlines to reconsider their flight paths and operations in the region. And this has seemingly resulted in an increase in overflights of Afghanistan.

Fighting between Ukraine and Russia resulted in tragedy. As Azerbaijan Airlines Flight 8243 to Grozny approached its destination on 25 December Russian air defences were repelling a Ukrainian drone attack. The plane eventually crashed in Kazakhstan, killing 38 people. Irrespective of the exact sequence of events, what we can be sure about is that the incident occurred in the context of an ongoing conflict between Russia and Ukraine.

Global conflicts also drove a major rise in GPS spoofing and jamming in 2024. Such incidents have been common around Egypt, Lebanon, the Black Sea, as well as near the Russian borders with Estonia, Latvia, and Belarus. GPS jamming has also occurred in Myanmar and on the border between India and Pakistan around Lahore, though less frequently.

Alongside and amid conflicts in 2024, hybrid or grey-zone warfare established itself as a security and safety challenge for many airlines. This has been particularly evident in Europe, where Russia-linked sabotage attacks have been most common. Several cases have targeted aviation, which many state and non-state actors perceive as a strategic sector when it comes to global supply chains. Sabotage attacks against cargo flights in mid-2024 – allegedly by Russian agencies – is only one such example. A spate of bomb hoaxes targeting Indian – and some international – airlines caused flight delays and disruption at airports.

Looking into 2025, wars in Ukraine and the Middle East continue. International stakeholders are keen to end these conflicts. But they will probably only be able to deliver a cold peace, prolonging animosity. Military exchanges – including missiles, drones, fighter jets, GPS spoofing and jamming – with little to no warning present a huge challenge to the civil aviation sector. There are several conflicts globally that could feasibly lead to such a scenario in 2025. Beyond ongoing and long-standing conflicts, in our Strategic Outlook 2025, we assess that armed conflict between Israel and Iran, Ethiopia and Somalia and civil conflict in Libya and South Sudan are all likely in 2025.

There are also several other pockets of instability with the potential to affect aviation in Asia this year. The two main flashpoints include Taiwan and the Korean Peninsula, where there is a high chance of a military escalation and sudden disruption to air operations. Pyongyang already fired a ballistic missile towards the East Sea on 6 January, highlighting what are increasingly frequent and expansive tests by the North. Similarly, China has been also stepping up its military exercises around Taiwan, which is another potential source of turbulent times.

9.2. Executive Brief: Global Aviation Security Challenges in 2025 – MedAire

Background

The aviation industry in 2025 operates within an increasingly complex and volatile security landscape. Persistent conflict zones, increasing overflight risks, rising geopolitical tensions, permacrisis and political transitions in key regions such as the Middle East, Eastern Europe, Asia Pacific, the United States, and Africa underscore the urgent need for a forward-thinking approach to aviation security (AVSEC). The industry must move beyond reactive measures, prioritising resilience, adaptability, and innovation to address current and emerging threats. By leveraging a combination of human resources and advanced intelligence

collection technologies, coupled with collaborative partnerships, aviation stakeholders can better manage risks, ensure operational continuity, and shape a sustainable future in an interconnected world.

Outlook on Global Aviation Security Risks

- **Middle East** – The Middle East remains critical for aviation security risks, driven by geopolitical rivalries and fragile conflict dynamics. While the Israel-Hezbollah ceasefire is temporarily reducing hostilities, its fragility highlights the region's volatility. A collapse of the ceasefire could lead to sudden airspace closures, GPS spoofing and interference, and heightened operational risks. Israel's intensified focus on countering Iran's influence, alongside Iran's advancements in missile systems and nuclear ambitions, compounds the complexity of the security environment. For aviation stakeholders, this necessitates proactive planning, including diverse intelligence collection and analysis and regional collaboration, to navigate congested airspaces and mitigate risks in high-threat zones like Yemen, the Red Sea, and other regional locations.

- **Eastern Europe** – Despite diplomatic overtures under the new U.S. administration, Eastern Europe's airspace remains volatile as tensions between Russia and Ukraine persist. While negotiations may reduce military operations temporarily, lasting resolution remains unlikely, with both sides leveraging tactical maneuvers to maintain strategic positions. The resulting instability in regional airspace, regular UAV and drone movements resulting in air defense systems and operatives being on constant high alert creates operational uncertainties and elevates overflight risks for air carriers to an extreme level. All of which underscore the importance of integrating advanced monitoring systems, diverse and integrated risk management modelling, and cross-border coordination to navigate this fluid security environment effectively.

- **Africa** – Africa's aviation security is shaped by political transitions and militant activity. Elections in Guinea and Gabon and persistent conflict between rivalries in Sudan present significant risks for airspace disruptions and accessibility to airports. Historical patterns of unrest during political transitions have demonstrated, most recently with Mali temporarily closing airspace following a military coup. Moreover, the security vacuum left by the withdrawal of international forces in the Sahel region has emboldened militant groups, increasing threats to aviation infrastructure and personnel. Key areas of concern include Burkina Faso, Mali, and Niger, where weak counterterrorism frameworks exacerbate vulnerabilities. A strategic approach prioritising regional collaboration, flexible contingency planning, and real-time intelligence sharing is critical to ensuring resilience and mitigating disruptions.

- **Asia Pacific** – Geopolitical tensions in Asia Pacific remain high, with intensifying military activities in the South China Seas and Taiwan Straits and with North Korea continuing non-kinetic provocations, such as missile tests and GPS spoofing. These actions disrupt airspace availability and operational continuity, particularly during periods of heightened U.S. cooperation with key regional players. Addressing these challenges requires strategic investment in resilient navigation systems, enhanced regional coordination, and advanced risk analytics and threat assessment tools to maintain safe operations in contested airspace.

Recommendations

To navigate these evolving aviation security challenges, the industry must adopt a forward-thinking, AVSEC-focused approach that emphasises the following:

- **Proactive threat detection and collection capabilities** – Utilise advanced platforms that integrate geopolitical data with

AVSEC-specific insights to proactively identify and mitigate emerging threats.

- **Technological innovation** – Consider technologies such as AI-driven capabilities, satellite-based navigation systems to counter GPS interference, and counter-drone measures to secure critical airspace and airport perimeters.

- **Global collaboration** – Strengthen partnerships with national and international organisations to help align AVSEC strategies, facilitate intelligence sharing, and standardise security practices across regions.

- **Scenario-based contingency planning** – Develop robust frameworks to adapt to diverse threats, including rapid response to global events by operational personnel and recovery protocols to maintain operational continuity. Test those scenarios.

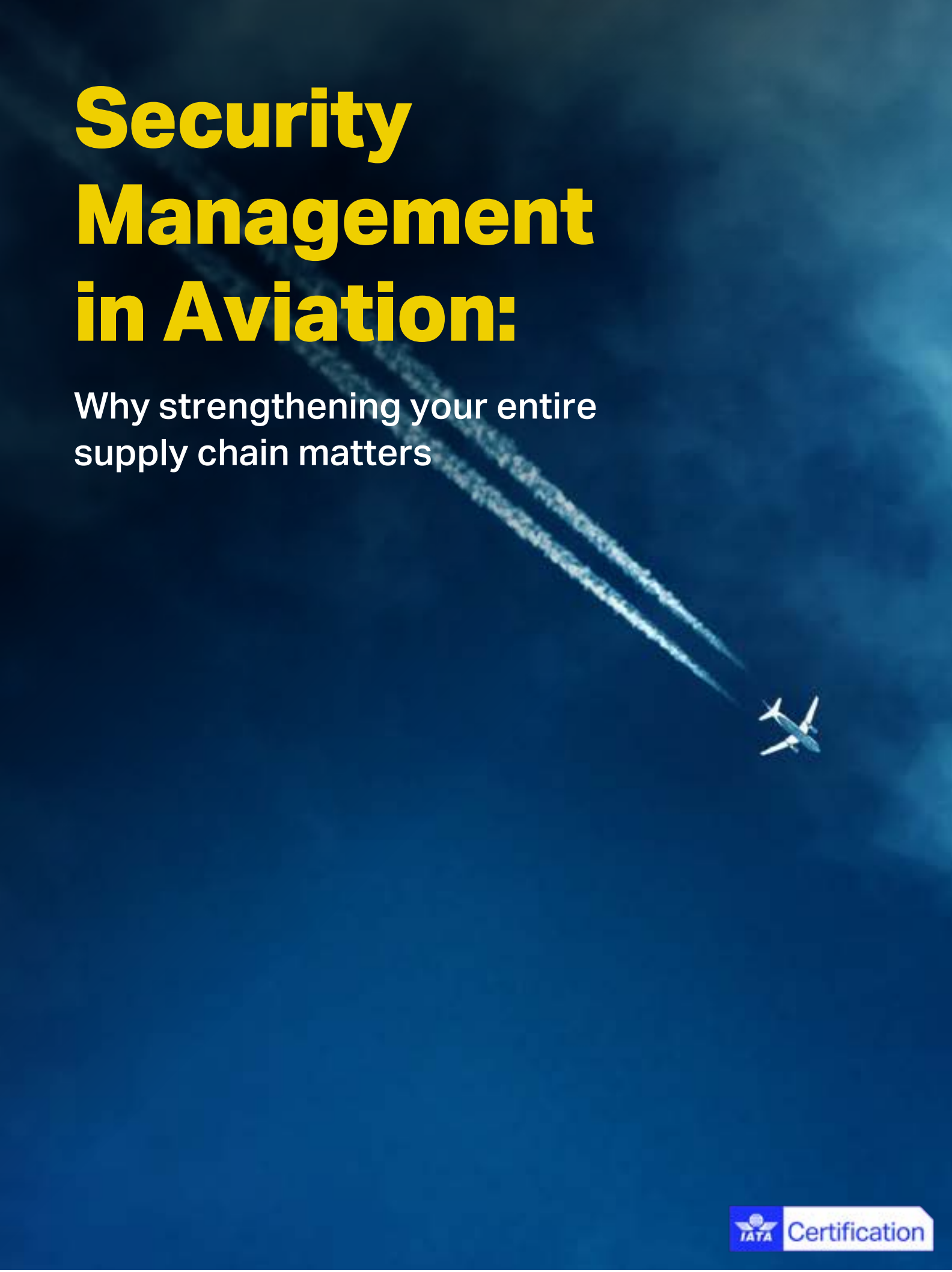
Conclusion

The security challenges of 2025 highlight the need for a proactive, strategic AVSEC approach. The aviation industry can effectively address evolving threats while ensuring safe and efficient operations by prioritising resilience, identifying, and detecting, leveraging advanced technologies, and encouraging global collaboration. This forward-leaning mindset mitigates risks resulting from current permacrisis and positions the industry as a leader in global security innovation, protecting lives, safeguarding passenger confidence and operational integrity in an increasingly volatile environment.

For more information, contact MedAire Security:
MedAireSecurity@medaire.com

Security Management in Aviation:

Why strengthening your entire supply chain matters



IATA Certification

The critical role of security management in aviation

Airlines, airports, and industry partners face constantly evolving physical risks and increasingly stringent regulatory requirements, making comprehensive security management essential. Maintaining effective security systems in this complex environment can be a challenge, even for the most vigilant organizations.

COMMON CHALLENGES IN AVIATION SECURITY INCLUDE:

OPERATIONAL CONTINUITY:

Security breaches can cause significant delays, disrupting the entire supply chain.

INCREASED COSTS:

Recovering from security incidents often leads to increased costs for protective measures and loss management.

REPUTATION MANAGEMENT:

A single security lapse can erode the trust and confidence that organizations have built with stakeholders.

The need for enhanced security is growing

Given the ever-changing nature of security threats within the aviation industry, stakeholders require a proactive and structured approach to effectively address and mitigate these risks throughout their operations.

IATA Certification

The solution: Security Management Systems (SeMS)

Security Management Systems (SeMS) provide a comprehensive, proactive framework for identifying and mitigating risks before they escalate. Rather than waiting for issues to arise, SeMS encourages continuous monitoring, assessment, and improvement, fostering a security culture that is both responsive and resilient.

KEY BENEFITS INCLUDE:

Risk-Based Awareness:

Develop strategies to anticipate threats and mitigates risks before they become critical issues.

Operational Efficiency:

Streamline processes to reduce the likelihood of costly disruptions.

Cost Savings:

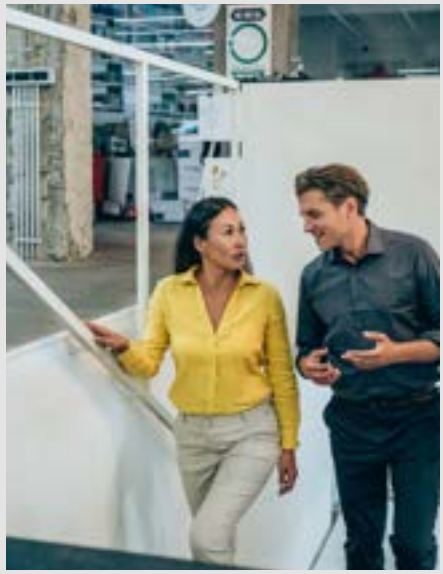
Develop preventative measures that reduce long-term expenses associated with security incidents.

Regulatory Compliance:

Build systems and processes to ensures adherence to evolving international security standards.

Continuous Improvement:

Create a company culture that prioritizes security excellence and can continuously adapts to new challenges.



IATA Certification

SeMS Certification and the future of aviation security

The SeMS certification program provides a framework that organizations can follow to enhance their security management systems. It aligns with IATA industry standards, ensuring a structured approach to proactive security management.

UNIFORM CERTIFICATION PROCESS:

Organizations across the aviation industry can adopt a standardized approach, promoting consistency and security throughout the supply chain.

RISK-BASED DECISION MAKING:

The certification emphasizes a proactive stance, making data-driven decisions that anticipate potential threats.

COMPLIANCE AND CONTINUOUS IMPROVEMENT:

The program ensures alignment with international guidelines and fosters a culture of improvement, crucial for maintaining robust security.

IATA Certification

Securing Every Link in the Supply Chain with SeMS

Aviation security breaches impact every aspect of the supply chain.

HERE'S HOW SEMS KEEPS IT SECURE.

GROUND HANDLING

- Ground services, such as baggage handling and maintenance, are vulnerable to security breaches (e.g., unauthorized access or tampered equipment).

→ SeMS Integration: SeMS ensures thorough background checks, secure operations, and continuous monitoring of equipment.

CARGO AND LOGISTICS PROVIDERS

- Cargo operations are vulnerable to tampering, smuggling, and theft.

→ SeMS Integration: SeMS offers real-time tracking, monitoring, and secure handling of goods, reducing risks of tampering and theft.

AIRLINE HUB

Airlines - Ensure passenger, staff, and cargo safety with proactive risk management.

CATERING AND INFLIGHT SUPPLIES

- Inflight catering and supply chains can be compromised if security is not stringent (e.g., food tampering).

→ SeMS Integration: SeMS guarantees the secure delivery and storage of inflight supplies through risk assessments and supplier vetting.

SERVICE PROVIDERS

- Outsourced services like cleaning, fueling, or security pose potential vulnerabilities.

→ SeMS Integration: SeMS ensures contractors comply with the airline's security policies through rigorous oversight and security audits.

Security Benefits Summary

- Risk Reduction
- Enhanced Compliance
- Improved Operational Efficiency
- Cost Savings
- Continuous Monitoring

IATA Certification

The impact of a proactive SeMS strategy

Implementing a proactive Security Management System is crucial for organizations looking to safeguard their operations, reputation, and stakeholders. With SeMS, the aviation industry can move towards a more efficient, cost-effective, and resilient approach to security that strengthens the entire supply chain.

CONTACT US

IATA Certification