IATA Annual Security Report

2023 Edition

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.

This Publication is the property of IATA and is protected under copyright. The Content of this Publication is either owned by or reproduced with consent or under license to IATA. This Publication and its Content are made available to you by permission by IATA, and may not be copied, published, shared, disassembled, reassembled, used in whole or in part, or quoted without the prior written consent of IATA. You shall not without the prior written permission of IATA: re-sell or otherwise commercialize, make mass, automated or systematic extractions from, or otherwise transfer to any other person or organization, any part of this Publication and its Content in whole or in part; store any part of this Publication, or any Content, in such a manner that enables such stored Content to be retrieved, manually, mechanically, electronically or systematically by any subscriber, user or third-party; or include it within, or merge it with, or permit such inclusion in or merge with, another archival or searchable system.

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.

1. Introduction

In 2022, IATA published its first Aviation Security Trend Report highlighting the top 5 Aviation Security challenges for the year. Looking forward, the reporting effort in 2022 served as the catalyst for a more generic, wholistic and detailed annual report on all security related efforts. Thus we present the inaugural **IATA Annual Security Report**[1], which is intended to become an annual publication complementing the security related sections of the broader IATA Annual Report and the IATA Economics team publication on Heightened Policy Uncertainty in 2024.

Looking back at the 5 main areas highlighted in the 2022 report, it is clear most if not all were, to a greater or lesser degree, pertinent to the ongoing aviation security debate and in some ways, however 'obvious' they may have seemed to some, insightful. The below are collection of macro issues, presented and discussed in no specific order.

1.1 Geopolitical Risks and Conflict Zones

No doubt the ongoing situation in Ukraine, and more recently events in the Middle East and Southern Levant, in addition to new and emerging conflicts within Africa have resulted in an increasing awareness of geopolitical risk. The IATA Aviation Security Trend Report was not unique in flagging or acknowledging such risks, from a forward-looking perspective, but 2023 has been a clear and present reminder, that geopolitical risks and conflict zones, particularly those with an ability to grow and escalate in size, scale, and geographical spread, must remain ever present on aviation focused risk registers.

1.2 Cybersecurity

As described in this report, cybersecurity persists as a paramount concern in addressing and responding to cyber threats and foreign interference targeting critical infrastructure. Both regulatory and industry stakeholders engage in ongoing dialogues, collaboratively identifying and endorsing recommended best practices. Simultaneously, efforts are being made to formulate and implement timely, effective, and proportionate mitigation measures based on a cohesive strategy. Throughout 2023, IATA has observed a range of cyber-attacks targeting information technology (IT) systems, a dearth of disclosure regarding operational technology (OT) vulnerabilities, the exploitation of cyber means for foreign interference, and a substantial surge in the adoption of machine learning and artificial intelligence (AI) approaches. The intricacies of the cyber challenge, intertwined with geopolitical risks and conflict zones, are anticipated to persist as a prominent agenda item in aviation security discussions for an extended period.

1.3 Civil Protests

It does appear that civil protests, directly targeted at civil aviation, either as the primary focus of protestors frustrations or as a convenient and media conscious disruptive backdrop to wider issues they wish to articulate and expand upon, do appear to have subsided somewhat since the 2022 Aviation Security Trend Report was first published. That said, civil protests are far from a thing of the past and recent geopolitical events have certainly appeared to bring to the forefront the idea of mass protest, which has in some cases, led to civil disobedience and unrest. It can also be argued that indirect disruption to civil aviation operations has morphed from a largely direct and personal degree of engagement (mass protests in and around aerodromes for example) into a more individualistic, impersonal, targeted and arguably more disruptive method e.g., bomb threats, typically hoax in nature, to individual flights, aircraft operators and/or aerodromes. As with most

[1] Content for this report has been sourced from our Strategic Partners, interviews with IATA personnel and internal reporting documentation.

threats, while the primary vector may remain relatively consistent, the individualist methodology can and does typically adapt over time.

1.4 Supply Chain Risks

As stated in the 2022 Aviation Security Trend Report, supply chain risks persist and are at times exacerbated by one or more contributing factors as detailed within this IATA Annual Security Report. It is difficult to imagine a scenario where geopolitical upheaval, armed conflict, civil protests, cyber security incidents and/or natural disasters does not negatively impact some elements within the supply chain, especially where the 'just-in-time' supply concept is an increasingly critical element of the business-to-business (B2B) and business-to-customer (B2C) concept of operations. As the world returns to a degree of normality post-pandemic it is possible that some risk managers may become less conscious of and alert to supply chain risks – but history has shown us that the impact of negative consequences are felt the greatest when we are least prepared.

1.5 Natural Disasters and Pandemic Risk

There is an increasingly collective conscious of impacts to the environment. Government and industry are taking ever greater steps, both voluntarily and because of growing legislation in this area, to minimise the potentially negative and harmful impacts some of our personal and professional decisions may have in that regard. The degree to which we are all seeing natural disasters play out in the media highlights to us all not just the potential risk to our planet but also the extent to which aviation and aviation operations can be affected. Natural disasters are a phenomenon (fires, floods, storms, droughts, extreme non-typical temperatures etc) and will arguably continue to feature on risk registers. They require a comprehensive and cohesive set of mitigations to ensure operational impacts remain manageable.

The COVID-19 pandemic has underscored the imperative for all organizations to reassess their strategies in the face of pandemic risks. Not least spending the time to evaluate the way in which civil aviation was impacted both in terms of passenger and cargo operations. No doubt global interconnectedness has magnified the impact on economies, emphasizing the need for resilient healthcare systems, diversified supply chains, and robust digital infrastructure. The accelerated adoption of technology and remote work has become pivotal for business continuity.

Some of the lessons learned that have since been documented highlight the significance of proactive planning, data-driven decision-making, and collaboration between public and private sectors. Characteristics of a fully functioning risk management system. Integrating these insights into strategic planning will empower organizations to navigate future crises, safeguard operations, and contribute to global resilience.

1.6 Summary

IATA cannot claim to have foreseen all of the 2023 eventualities within the 2022 Aviation Security Trend Report, just as we do not assume to have a unique insight into 2024, but we hope that the contents of this inaugural IATA Annual Security Report highlights the endeavours of our staff, our members, our Strategic Partners and the wider aviation community, including all of the regulators who actively look to adopt an open, engaging and pragmatic approach to collective information gathering, review, discussion and mitigation adoption.

Some may argue that the 5 issues highlighted in the 2022 Aviation Security Trend Report were reasonably generic, indeed commonly held beliefs, but for some they were hopefully insightful in that they helped to educate and inform wider debate and, directly or indirectly, contribute to organizational risk assessment considerations. At the very least it was hoped that it would provide a useful means of reenforcing existing thoughts and/or assist in helping security managers to better articulate and present their own concerns and security considerations.

It is fair to say 2023 has been in many ways a positive and rejuvenating year, not least as we collectively started to emerge from the consequences of a global pandemic. That too brought challenges, particularly in respect of how we all looked to re-start our industry, reenergise our organisations, grow our businesses and re-awaken our senses. Unfortunately, 2024, across several fronts, is already starting to look like another challenging period, but with a sound, sensible, proportionate, and pragmatic collective approach to problem solving, IATA remains confident our industry, and all those that support and engage with it, will continue to deliver safe, secure, and sustainable aviation services.

2. Executive Summary

This report is modelled on the 60-year publication of the IATA Annual Safety Report recording industry performance across a range of safety performance indicators. Whilst this annual security report aims to discuss and highlight key areas of aviation security, it is different in the sense that the inaugural edition aims to provide a comprehensive readout of IATA's global efforts within and across the aviation security domain. Additionally, this report recognizes that safety and security are risk management partners with different approaches and outcomes. More broadly, aviation security requires acceptance of the limitations in predictive risk values and vulnerabilities are omnipresent that require ongoing collaboration and innovation.

It is arguable that the current approach to aviation security is constrained by legacy thinking, which leads to incremental changes rather than innovative modelling. While industry and regulators typically iterate on existing measures, there is a growing recognition that starting afresh could yield better results. Given today's advanced screening technologies, evolution of AI, and an improved understanding of threats, we envision a more efficient and secure aviation system.

"...aviation security is constrained by legacy thinking".

A radical re-think could involve assembling a diverse group of experts to re-evaluate risks and develop a tiered security system that acknowledges varying capabilities whilst engendering new levels of innovation. The envisaged system would not be bound by a one-size-fits-all approach but recognize different levels of security excellence, allowing for seamless operations within security tiers and flexibility for entities to move between tiers as they upgrade or change their policies and practices.

Ultimately, a series of questions are being posed whether we should continue to evolve from an outdated foundation or whether it is time to start from a new conceptual baseline? A new commonly understood and accepted baseline would limit the knee-jerk reactions to the latest threat and take on a systems resilience posture towards the known and unknown of threats.

Can we re-imagine global aviation security standards, building mutual recognition at a far more granular level that moves beyond only State to State agreements? Yes, by supporting and replacing, or at least supporting, binary compliance, oversight, and quality assurance mechanisms with a more dynamic and outcome focussed approach based around qualitative, timely and evidence-based Security Management Systems (SeMS).

Most notably the outcomes from IATA's annual Global Passenger Survey (GPS) continue to provide a unique basis for why a rethink needs to be considered. Starting with the passenger security checkpoint. Passenger experiences at the checkpoint continue to rank, year-after-year in the top three dissatisfaction areas for civil aviation. What's more, is that most checkpoints are far from clear adoption of risk -based, differentiated screening protocols. A light touch security for low-risk passengers and additional measures for those who activate alarms is achievable.

IATA continues to support progressive innovation in developing open AI-based screening systems and pilot initiatives in terms of remote and self-passenger screening. However, IATA was disappointed by the International Civil Aviation Organizations' (ICAO) Electronic Bulletin (EB) release on liquids aerosols and gels (LAGs) in May 2023. The EB reinforced the recommendation that LAG measures are still required. Paradoxically, LAGs measures are not an ICAO Annex 17 standard, nor has any further generic threat and risk guidance advice been provided via the latest version of ICAO's Risk Context Statement (Doc 10108-Restricted), to justify

such a release. We continue to work with the respective groups in ICAO to ensure risk-based and differentiated screening approaches ensue.

Finally, the 2nd Edition of the ICAO Global Aviation Security Plan (GASeP) (Doc 10118) to be released in 2024 continues to serve as the *"guiding light"* of aviation security efforts. The second edition importantly builds upon the September 2016, United Nations Security Council Resolution (UNSCR) 2309 (2016) – *threats to international peace and security caused by terrorist acts,* a swath of key learnings stemming from COVID-19 experiences and ongoing amendments to Annex 17.

IATA persists in advocating for a proactive strategy that goes beyond simple consultation and encourages collaboration. Given the evolving threats, aviation security should not be limited to a fixed set of protocols but should function as a dynamic system that consistently adjusts to safeguard the integrity of civil aviation. There is still ample exploration needed to understand the interconnected dynamics between security and safety fully. The forthcoming release of the 2nd Edition of the ICAO GASeP is anticipated to take the lead in addressing these aspects and many more.

3. Glossary of Terms

Acronym	Description
AI	Artificial Intelligence
AOSP	Aircraft Operator Security Program
ARF	Aircraft Recovery Forum
ASPAC	Asia Pacific
ASTF	Aviation Security Trust Framework
AVSEC	Aviation Security
AVSECFAL	Aviation Security Facilitation
AVSECP	Aviation Security Panel
B2B	Business to Business
B2C	Business to Consumer
BoG	Board of Governors (IATA)
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
EASA	European (Union) Aviation Safety Agency
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
GASeP	ICAO Global Aviation Security Plan
GRH	Ground Handling Operations (part of the IOSA scope)
GTRF	Geopolitical Risk Task Force
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IDX	Incident Data eXchange (IATA)
IOSA	IATA Operational Safety Audit
IRM	Integrated Risk Management
IRRM	Integrated Risk and Resilience Management
IOSA	IATA Safety Audit Program
iSARP	IOSA Standards and Recommended Practices
ISM	IOSA Standards Manual
KCs	Known Consignors
KPIs	Key Performance Indicators
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
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
TFP	Trust Framework Panel (ICAO)
TSA (US)	US Transportation Security Administration
UN	United Nations
UNSCR	United Nations Security Council Resolution
USAP	Universal Security Audit Programme (ICAO)
WGTR	Working Group on Threat and Risk (ICAO)
WSOC	World Safety and Operations Conference (IATA)

4 Summary Overview for 2023

4.1 Global Security Overview[2]

Geopolitical competition will almost certainly remain a major source of risk and volatility for the aviation sector in 2024. Ongoing conflicts that have negatively impacted airspace globally are highly likely to persist. These include the conflicts in Ukraine, and between Israel and Hamas in Gaza. Civil and interstate military tensions in many parts of Asia, Africa and the Middle East are as high as they have been for decades.

Dragonfly Intelligence assesses that almost a third of countries worldwide have a worsening security and stability outlook over 2024, including China, France, Germany, North Korea, Pakistan, and Russia. Whereas only 11 countries are likely to see an improvement, among them Ethiopia, Syria, and Türkiye. For most countries, the overall stability trajectory we assess is broadly consistent, albeit for many this means a continuation of volatility.

4.1 Aviation Security and Cybersecurity

Through the leadership and guidance provided by the IATA Security Advisory Council (SAC) - one of nine Advisory Councils under the IATA Board of Governors - IATA aims to lead, influence, constructively challenge and actively support efforts that seek to safeguard the aviation industry, the travelling public and those that work in it. We achieve this is an effective and timely manner, whilst also enabling safe and secure sustainable growth.

It is imperative that civil aviation be effectively protected against harmful and unlawful acts through a set of comprehensive, proportionate, timely, efficient, and interlinked sets of physical, procedural, technical, and digital security strategies. These strategies must be positioned to strengthen confidence in existing and evolving mitigation measures, systems, and approaches together with the outcomes that are achieved. To that end IATA will continue to lead and actively champion improvements designed to close gaps and vulnerabilities. Specifically, improvements may be realized via engaging in collaborative cross-border initiatives and associated regulatory reforms. Notwithstanding the imperative to remain responsive to new threat challenges, it is the goal is to minimize impacts from overly reactive and potentially disproportionate, time limited approach to policies, regulations, and/or extraterritorial requirements.

Appropriately framing current and reasonably anticipated macro-level challenges and opportunities is a fundamental strategic requirement, one which the SAC is committed to addressing via the creation and adoption of a clearly defined set of priorities (in no specific order):

- Minimizing airport infrastructure constraints in the medium and longer-term
- Mitigating overreaching, redundant and/or limited reciprocal regulatory requirements.
- Monitoring emerging, asymmetrical an/or less obvious security threats, both kinetic and digital in nature
- Increasing customer, shareholder, owner, and regulatory expectations resulting in continuing pressure from stakeholders to continually evolve industry performance and standards.
- Improving pre-decisional consultative and collective outreach of developing strategic and/or imminent reactive changes to security systems, processes, and postures.
- Develop strategies based purely on technology and technological solutions. Strategies should include a set of broad, holistic, interconnecting and mutually supportive measures which lead to desired performance, risk-based regulations, and security outcomes of a security system.

[2] Opening brief provided by Dragonfly Intelligence.

- Develop succession planning which mitigates the erosion of industry experience and expertise by preparing the next generation work force for the challenges ahead.

To meet these industry priorities, IATA will continue to adopt a forward-thinking, partnership-based working relationships with airlines, regulatory authorities, and other international organizations to meet these industry priorities. Although IATA's approach is primarily focused on strategic aims and objectives, it is also able to flexibly adapt to tactical and at times operational demands as circumstances and rising tide intelligence and pertinent information feeds dictate. Strategies must seek to mitigate vulnerabilities, identify, and track evolving threats and concentrate on high-risk focus areas in a timely and effective manner while supporting aviation sustainability, innovation, and effectiveness within a safe and secure framework.

IATA recognizes that its efforts and those of many other actors, including State level regulatory bodies, cannot rely on a "one-size-fits-all" approach but rather needs to adopt and utilize a proportionate, collaborative, information led and evidence-based methodology that is risk-aware but not risk-averse.

4.2 Message for Civil Aviation Regulators

Following the landmark UN Security Council Resolution 2309 (2016) on Aviation Security and the requirement for States to meet their obligations in the effective and sustainable implementation of ICAO Annex 17 standards.

IATA strongly encourages the regulators of States to ensure:

— The implementation of harmonized, sustainable, and proportionate baseline security measures.
— Support government and industry partners to limit reactive policy response and improve their readiness to manage emerging threats and/or vulnerabilities.
— New regulations are consistent and coherent and supported by appropriate guidance material.
— Support pilots in pursuit of smarter and faster next-generation aviation and border security solutions for all aspects of aviation – in accordance with UNSCR 2309 (2016) and 2396 (2017).
— Act promptly to ensure the facilitation and adoption of mutual recognition and the acceptance of supporting aviation security systems and associated components.
— Recognise Security Management System (SeMS) approaches with respect to risk-based oversight and proactive resolution of deficiencies. The deficiencies and the outcomes of ongoing, systematic, unresolved concerns are shared with aircraft operators.
— Appropriate and timely pre-decisional consultation and risk information is shared in a timely, and effective fashion, with all affected stakeholders.
— Security mitigation measures undergo a rigorous impact and cost-benefit analysis prior to being enacted.
— A holistic and integrated approach is taken to identify risk and vulnerability wherever possible, and pro-actively support and encourage industry mitigating measure innovation.

5 IATA Governance Groups and Work Plans Overview

5.1 Board of Governors (BoG) 2023 Targets

IATA's priority targets for 2023 were largely set by the IATA Board of Governors (BoG). A high-level overview can be accessed here - https://www.iata.org/en/about/priorities/. In terms of governance, IATA's security related priorities are guided and advised by the IATA Security Advisory Council (SAC).

5.2 Security Advisory Council (SAC)

The SAC work plan is based on the following guiding principles and outlined in preferred order:

Facilitate and inform improved airline security performance.

> Activities and initiatives that directly aim to increase and augment the ability of airlines to establish a measurement mechanism for their own data-driven security performance requirements and subsequent benchmarking as and when required.

Build external stakeholder trust and confidence in Security Management Systems (SeMS).

> Activities and initiatives that build upon IATA's tradition of SeMS in the face of evolving regulatory policy, growing recognition for risk-based outcome focused aviation security oversight, both within IOSA and in respect of State of Registry and foreign regulators requirements.

Increase security efficiencies.

> Identifying those areas in aviation security (technical, operational, and regulatory) that, when subject to the fullness of research and analysis, require a degree of reform and optimisation to be fit for strategically relevant purposes as interlinked with these guiding principles.

Enhance resilience and improve risk management capabilities.

> The adoption of a no-surprises approach when identifying and mitigating known and unknown kinetic and digital security risks. Furthermore, taking the steps necessary to better prepare and support industry when seeking to proactively manage and mitigate vulnerabilities, including reacting to rising tide intelligence situations and short notice emergencies via improved communication channels, contingency planning, and exercises.

The IATA SAC met twice throughout 2023 in Montreal, Canada and Hanoi, Vietnam, the latter alongside the IATA World Safety and Operations Conference (WSOC). The below is a high-level readout of key outcomes.

Checkpoint Screening - there is an observed international concern regarding checkpoint screening performance and detection of prohibited items. The SAC endorsed the use of IATA IDX for increased reporting so enable a more comprehensive view of empirical concerns.

Aviation Cybersecurity – IATA approach to aviation cybersecurity received full SAC support, emphasizing the IOSA proof-of-concept in later 2023/2024 in view of integrated risk management principals. Additionally, the SAC noted there is a need to improve transparency with Original Equipment Manufacturers (OEM), update aircraft log file guidance, and to integrate cyber provisions in future SGHA templates.

ICAO AVSEC Panel Working Group on Threat and Risk (WGTR) - the SAC recognized challenges for industry input towards influencing the deliberations of the ICAO WGTR. The SAC supported a potential co-located

WGTR meeting in Miami in 2024, allowing for SAC and GRTF viewpoints to be presented directly in view of a 2024 ICAO Risk Context Statement and General Assembly in 2025.

ICAO Annex 17 and Aviation Security Manual (Doc 8973) *changes* - the SAC noted that airlines continue to face difficulties in the implementation of changes to the Aircraft Operator Security Program (AOSP) and Station Supplementary Procedures (SSP) in ICAO Annex 17. The SAC urged IATA to increase its efforts in promoting and educating stakeholders about these changes. Noting this effort, the SAC reiterated its support for the digital aviation security framework in 2024 and the modernization of Doc 8973 with specific reference to hold baggage security arrangements.

One Stop Security (OSS) – the SAC noted apprehensions regarding the unilateral implementation of OSS measures between States, with a call for better multilateral coordination and data dissemination, prior to and during trials and implementation of OSS arrangements. New guidance on the Recognition of Equivalence (or OSS) are available on the ICAO public website, focusing on OSS during the last ICAO AVSEC and CYSEC Week 2023

Geopolitical Risk - the SAC supported the Geopolitical Risk Task Force's (GRTF) work plan, specifically addressing the risks arising from congested and constrained airspace resulting from disruption and conflict. The SAC supported leadership awareness for an OAC-coordinated BoG information paper (IP) in this regard.

5.3 Cyber Management and Resilience Working Group (CMRWG)

The CMRWG progressed its workplan in 2023, primarily in connection to the BoG target identified on IATA industry priority for 2023 in reference to strengthening airlines capacity to address cyber security risk and emerging regulation with respect to aircraft operations.

The CMRWG work plan is broadly arranged around these key areas:

- **IOSA Cybersecurity for Security, Safety and Airworthiness (CSSA) –** multiyear roadmap of iSARP proposals capitalising on existing cybersecurity iSARPs in the last edition of the IOSA Standards Manual (ISM).

- **International Advocacy on standards and regulatory development** – CMRWG provides guidance to IATA on interventions and comments in relation to proposals/interventions at international multilateral forums such ICAO Cybersecurity Panel, ICAO Trust Framework Panel (TFP) and other panels. This is inclusive of EUROCAE/RTCA industrial standards arrangements.

- **International Incident and Crisis Management Framework** – progressing a framework accessible to all stakeholders of the civil aviation supply chain, in the event of an international cyber incident & accompanying crisis management arrangements.

- **Modern Airlines Retailing** - A work plan item to develop/review cybersecurity requirements and associated matters for enterprise systems and data. This package primarily is scoped to cover commercial and passenger processing systems that have implications on passenger data from a privacy and cybersecurity perspective.

5.4 Geopolitical Risk Task Force (GRTF)

The Geopolitical Risk Task Force (GRTF) is comprised of 19 members from all regions except Central and South America. The GRTF report met twice in 2023 reporting to the Security Advisory Council on the following:

- The IOSA Standards Manual (SEC 4.1.1) requires airlines on the registry to have a process in the development of risks, vulnerabilities, and response measures. While the IATA SeMS Manual and the 2nd edition of ICAO DOC 10084 do not specifically offer technical risk assessment guidance in relation to airspace/overflight arrangements, the GRTF aims to standardize the risk assessment processes for airlines, by empirically developing guidance to identify the risk demands during flight planning, of airspace that will provide a safe/secure operating environment. The current practice for sharing and creating rapid/urgent information on existing/evolving conflict zones and related airspace closures/restrictions is via the NOTAM system. Unfortunately, information related to airspace disruptions contained in the existing NOTAM format, is not standardized, and only published by a limited number of States. In this context, the GRTF is reviewing NOTAM policies and processes in view of security risks arising from conflict zones.

- The IATA hosted information sharing "Baseline Call" is a high-level activity for States, airlines, and industry partners taking a "no-surprises" approach to risk management. The strategy of the Baseline Call is for stakeholders to collaborate in an unclassified setting and achieve broad awareness of emerging/active threat/risk concerns to civil airspace and airports exposed to militarized hostilities. In this context, the GRTF is reviewing the current scope of the Baseline Call with the view of establishing criteria and a process for public private information sharing information. Moreover, develop a more targeted product in terms of geographic and risk concerns, encourage wider participation through increased awareness for airlines, ANSPs, and other working groups such as the SSCC and the ICAO Working Group on Threat and Risk.

- The GRTF has communicated with the ICAO WGTR as well as the Safer Skies Consultative Committee (SSCC) led by Canada and the Netherlands. Given the focus of each group, the intent is to ensure these groups receive airline contribution into their work products related to the impact threats/risks may have on airspace capacity.

5.5 Cargo Security Working Group (CSWG)

The Cargo Security Working Group (CSWG), made up of 15 members, reporting to the IATA Cargo Border Management Board (CBMB) met twice in person in 2023. Key summary items as per below:

- They are leading a joint initiative between US Transportation Security Administration (TSA) and European Union (EU) on air cargo security, with ongoing actions aligned with the CSWG multi-year work plan.

- Proactive in identifying emerging regulatory requirements and initiating consultations.

- CSWG is aiding in the adoption of ICAO Annex 17 related to air cargo security, including the phase-out of the account consignor process.

- A workshop on Consignment Security Declaration (CSD) was conducted in Q3 of 2023 to support revisions and promote electronic practices.

- The group continued to provide security related advice for risks associated with transporting lithium batteries, providing security supply chain advice, a key target for the 2023 IATA Board of Governors. Enhance information sharing for risk assessments, especially regarding the safe carriage of lithium batteries.

- Support the development of further guidance and best practices to members on various topics like electronic Consignment Security Declaration, procedural changes, and screening performance.

- Support implementation of Security Management Systems (SeMS) in the air cargo supply chain, promoting a risk-based security approach and the intersection of safety and security, particularly concerning Dangerous Goods.

5.6 SEC Task Force (SEC TF) (IOSA)

According to its current Mandate (2023-2026), the IOSA Security Task Force (SEC TF) is the reporting to both the IOSA Oversight Group (IOG) for the IOSA activities and the Security Advisory Council (SAC) for other security activities.

The primary responsibility of the SEC TF is to ensure the continuous update and improvement of the IOSA Standards and Recommended Practices (ISARPs) in the Security Management discipline of the IOSA Standards Manual (ISM), as well as the ongoing interpretation of SEC ISARPs.

A second responsibility is to support the SAC in the development of security policies, position papers, and vision and to support IATA in the development and update of relevant security related guidance material, training certification tools or any other product and service that may be relevant, including technical support to IATA's contributions in the relevant IAO aviation security Working Groups and Task Forces.

In the context of its extended mandate that SEC TF assisted IATA Security in the launch of a comprehensive SeMS survey for all IOSA registered airlines with the objective of assessing the level of comprehension and maturity of the SeMS concept. The first comprehensive SeMS Survey (Nov 2022) has been followed up by two more targeted Flash Surveys (in February and March 2023) to further develop some of the key results of the initial such as the magnitude of the current outsourcing of security operational functions.

The survey results demonstrated that almost all IOSA registered airlines (more than 90% according to the surveys) use External Service Providers (ESPs) for undertaking more than twenty-five (25) security operational functions contained in the GRH, CGO and SEC ISM sections. The need for monitoring and oversight over ESPs has been an ICAO Annex 17 requirement since 2010, supported by a new Standard in 2020.

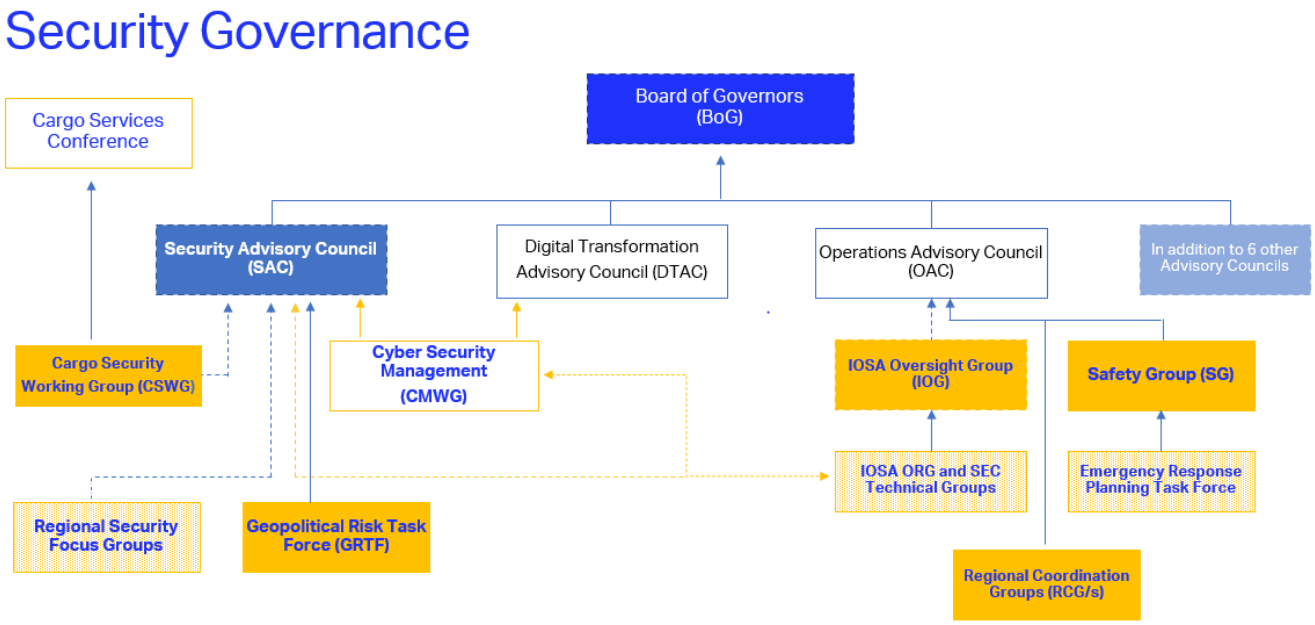
The SEC TF advised that the elevation of ORG 1.6.1 and SEC 1.11,1A to a Standard for the selection of ESPs, combined with the introduction of a new Recommended Practice SEC 1.11.3 encouraging ESPs to follow the very same SeMS key elements that are applicable to the operators, would reinforce a better harmonization and generate potential savings for the Quality Assurance and Quality Control functions that are reflected in the ORG Subsection 2.2 - External Monitoring and SEC Subsection 1.11 - Quality Control of Outsources Operations and Products for the 17th edition of ISM.

It should be noted that due to a change in the ISM cycle, ISM/17 to be published in April 2024 with an effective date in January 2025.

More than twenty (20) existing security related ISARPs and associated Guidance Material (GM) have been adjusted in ISM/17 and the work continues with an in-depth analysis of the ISM Sections GHR and CGO for ISM/18 considering the results of a third survey on ground and cargo operations.

Several SEC TF members actively participated in the development of new toolkits for assessing SeMS in ESPs that have been presented during the IATA Security Forum 2023 (see below in this report) and will be evaluating those tools during a testing phase finishing in March 2024. The testing of SeMS for ESPs toolkit will also help in the potential redrafting of GRH and CGO ISARPs and associated GM for ISM/18, as well as in the redrafting of

the IATA SeMS Manual (2025) for enlarging the audience to potentially any entity in the aviation ecosystem that could become an ESP for civil aviation operators.



IATA SAFETY ISSUE HUB

Discover a one-stop shop for information, guidance material, and risk assessments to help airlines ensure their safety and security management systems are top-notch.

+70
Safety Issues Identified

+ 200
Guidance Material docs

A self-service digital platform to gain access to global aviation safety and security issues, risk assessments, and mitigation guidance material

Visit the Hub to stay tuned on critical safety/security issues across regions and operational domains.

Let's join efforts!

Sharing knowledge and best practice elevates safety and security management standards.

The Safety Issue Hub

Share An issue

IATA

6 International Regulatory Overview

6.1 Informal ICAO Council Security Briefing

In September 2023, the IATA Director, Aviation Security & Cyber, was provided the opportunity to deliver an informal briefing to the ICAO Council on security incidents and available data. The below is a summary of key points:

- Addressed the growing concerns in civil aviation security, particularly related to unruly passengers, bomb threats, and cyber-attacks from an airline industry perspective.
- IATA recognized the continuous efforts by ICAO and others to maintain safe skies and acknowledges that security breaches impact the entire global community.
- Acknowledged the limitations in security incident data due to governance issues and emphasizes the need for international cooperation and better reporting protocols.
- Emerging threats like drone interferences and undeclared dangerous goods in air cargo were also highlighted, with a call for improved intelligence sharing to support airlines' risk management.
- Emphasized the need for globally harmonized implementation of standards and a comprehensive review of the global aviation security model, seeking to understand differing interpretations across states and aiming for transparency in the audit process.
- Emphasized the use of data from IATA's Incident Data eXchange (IDX) program to discuss the prevalence of bomb threats and unruly passengers' incidents, noting significant data limitations.
- There were 97 reported bomb threat incidents between January 2021 and August 2023, with a majority not followed by immediate investigation or arrest.
- A total of 20,301 reports of unruly passengers were recorded from January 2021 to December 2022, with an increase in the incident rate from 2021 to 2022.
- Despite no cyber-attack compromising flight safety systems to date, cybersecurity in aviation is a growing concern due to the sector's reliance on digital systems.
- The airline industry's technology adoption increases vulnerability to cyber threats like other sectors, with IATA calling for the incorporation of cyber occurrence reporting into its IDX program.
- IATA identifies the challenges airlines face due to the IT supply chain vulnerabilities and the withholding of cybersecurity status by suppliers under the pretence of protecting intellectual property.
- The brief concludes by urging the mandatory reporting of all security occurrences and incidents and advocating for industry participation in working groups to help shape accurate threat and risk assessments.
- IATA called on ICAO to play a pivotal role in creating guidelines, setting standards, and facilitating best practice sharing to maintain a resilient and secure global aviation system.

6.2 ICAO AVSEC Panel

IATA's active participation in the ICAO Aviation Security Panel (AVSECP) and its Working Groups and Tasks Forces is essential for promoting Industry views across ICAO reference materials. Specifically, when deliberating ideas that may negatively impact civil aviation operations, and/or preparing the industry when new requirements are decided. This preparation encompasses adjustments in the ISM and IATA Manuals, but also in the development of guidance or tools that could help in the implementation of new ICAO provisions or reduce the potential negative impact with non-harmonization.

IATA's advocacy and active participation in the last Amendments 17 (2020) and 18 (2022) to the Annex 17 cycle reach the following goals, among others:

- New Standards for Aircraft Operator Security Programme (AOSP) and Supplementary Station Procedures (SSPs) that should help in the conformity level of Annex 17 Standard 3.3.1
    - New ICAO public guidance material on AOSP/SSP have been developed with IATA's input.
    - Note that the ICAO Universal Security Audit Programme (USAP) has adjusted its assessment tools for better reflecting the effective implementation of several Standards, including Standard 3.3.1 which is jump from 30% effective compliance (2022) to 70% (end 2023) because of the new calculation.
- ICAO Annex 17 Standard 3.4.9 (2020) then 3.5.3 (2022)[3] on the oversight function of operators over their external service providers.
- Standard 3.4.2[4] (2022) for the assessment of competencies for all personnel with security functions during initial and recurrent training.
- Development of new ICAO public guidance material on the reporting of occurrences and incidents also developed with a strong IATA input for ensuring consistency with IATA IDX taxonomy, but also the taxonomy pushed with EASA and ECAC.

Amendment 18 to Annex 17 (2022) is mature and covers most of the needs for implementing robust aviation security systems in ICAO Contracting States, and the effective implementation of ICAO Annex 17 Standards should remain the highest priority for States. As a result of ICAO USAP results, in mid-2022 ICAO issued a State Letter surveying for root causes of issues with implementation of Annex 17 requirements. USAP results identified that only 50% of States have reached an effective level of implementation, despite the Standards being introduced over 15 years ago. The analysis of the results and proposed course of action with AVSECP entities is an on-going activity,

In this context, some discussions should still take place in the relevant AVSECP Working Groups (WG) such as the WG on Annex 17, the WG on Air Cargo Security or the WG on Guidance Material for further improving both the provisions in Annex 17 and the relevant guidance material contained in the ICAO Aviation Security Manual (Doc 8973). The discussion topics are the following ones:

---

[3] "…Each contracting state shall ensure that each entity responsible for the implementation of relevant elements of the national civil aviation security programme periodically verifies that the implementation of security measures outsourced to external service providers is in compliance with the entity's security programme."

[4] "…Each contracting state shall ensure that all aviation security training programme for personnel with responsibility under national civil aviation security programme include an assessment of competencies to be acquired and maintained for initial and recurrent training."

- → Alignment of Annex 17 Standards 4.6.2[5] and 4.6.5[6] regarding "other entities" for clarifying if there is a need for such "other entities", and if yes, propose the development of proper guidance material in Doc 8973 for explaining what those entities are and what is expected from them (such as in Appendices 31 and 32 for Regulated Agents RAs and Known Consignors KCs).
- → Discussion on the preferred use of "electronic security status" in Standard 4.6.8[7]
- → Full review of Annex 17 Chapter 4.5 that has been stopped during Amendment 18 process due to lack of time.
- → Introduction of "security occurrences" and "security incidents" in Standard 5.1.6, following the new ICAO guidance (public, 2022) as well as the recent discussions taking place in the European Union (Commission) and EASA.
- → Regarding SeMS in Standard 3.5.3, we will inform the AVSECP on the IATA development with the SeMS for ESPs toolkit, its testing phase, and the potential consequences in IATA Manuals, Documents and Programs in 2025-2026.

IATA continues to enjoy the collaborations with partner "observer international organizations" at ICAO and contributes to the co-sponsoring of a range of industry led interventions. I.e. SeMS, Air crew screening and conflict zones with the Security Committee of the International Federation of Air Line Pilots Associations (IFALPA).

IATA supports the revised and updated 2nd Edition of the ICAO GASeP, which IATA hopes will build upon the success of the original GASeP concept, helping to reinvigorate and raise the profile of aviation security capacity development and associated improvement initiatives.

Finally, IATA continues its internal coordination with cross-referenced topics such as the potential security risks associated to the carriage of some dangerous goods items (such as batteries) that are intentionally and unlawfully introduced in aircraft via undeclared (or miss-declared) consignments and that could cause damage to an aircraft in service, rendering it incapable of flight, or which is likely to endanger its safety in flight. Such cross-referenced topics are discussed in different ICAO Panels, and WGs, thus necessitating a close and proactive coordination for aligning Industry positions, adjusting IATA Manuals, Documents and Programs, particularly with the extending pace for adjustment of guidance and provisions by ICAO.

6.3 ICAO Cybersecurity Panel

IATA actively engages in key cybersecurity initiatives, holding observer status in both the ICAO Cybersecurity Panel (CYSECP) and the Trust Framework Panel (TFP).

The current work plan of the ICAO CYSECP is separated into two sub-groups focusing on the development of universal risk assessment Methodology guidance, incident sharing and reporting, and guidance material on threats and risks. Similarly, the ICAO TFP work plan is supported by sub-groups focusing on key issues such as

[5] "…Each Contracting State shall establish a supply chain security process, which includes the approval of regulated agents and/or known consignors, if such entities are involved in implementing screening or other security controls of cargo and mail."

[6] "…Each Contracting State shall ensure that operators do not accept cargo or mail for carriage on an aircraft engaged in commercial air transport operations unless the application of screening or other security controls is confirmed and accounted for by a regulated agent, a known consignor, or an entity that is approved by an appropriate authority. Cargo and mail which cannot be confirmed and accounted for by a regulated agent, a known consignor, or an entity that is approved by an appropriate authority shall be subjected to screening."

[7] "…Each Contracting State shall ensure that cargo and mail that has been confirmed and accounted for shall then be issued with a security status which shall accompany, either in an electronic format or in writing, the cargo and mail throughout the secure supply chain."

digital Identity, the ICAO Information Security Manual (ISM) which contains over 600 provisions. IATA is deeply involved in providing technical support and guidance across these efforts.

IATA continues to lobby for the avoidance of isolated development of cybersecurity SARPs and guidance as iterated WP/64, presented at the 41st General Assembly. IATA emphasizes the need for an integrated and coordinated approach across ICAO working bodies, promoting a cross-discipline, Security by Design methodology to minimize duplication and ensure harmonization.

At the Second CYSECP meeting in June 2023, IATA presented WP/16 proposing the creation of a new Annex 20 on Cybersecurity. Recognizing the pervasive impact of cybersecurity on aviation stakeholders, IATA advocates for consolidating cybersecurity SARPs in a dedicated annex.

In summary, IATA actively shapes and influences cybersecurity strategies within the aviation industry, fostering collaboration and advocating for a streamlined approach to cybersecurity provisions.

6.4 Safer Skies Consultative Committee (SSCC) & Safe Skies Forum 2023

IATA participated in several meetings held consecutively related to conflicts and airspace disruptions in June 2023. The meetings were coordinated by the Safer Skies Consultative Committee (SSCC). In addition to an in-person SSCC meeting, the 3rd Safer Skies Forum was held as well as a meeting of the Expert Group on Regional Conflict Zones (EGRICZ). The Final Report - 3rd Safer Skies Forum is publicly available.

During these events, in collaboration with the SSCC, IATA supported the concept of a program that will provide workshops/training on threat/risk mitigations related to conflict zones. However, the IATA concept included a recommendation that alternative funding options be sought to ensure appropriate level of training and workshops could be delivered against measurable key performance indicators.

One of the key deliverables targeted by the SSCC was to update and amend ICAO Document 10084, *"Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones"*. Given IATA's experience on this topic, IATA ensured airline perspectives were incorporated in what is traditionally known as a regulator focused document. The document will be helpful in assisting airlines when conducting their individual and collaborative Risk Assessments.

Link to Doc 10084: Doc.10084.Third edition.pdf (icao.int)

To promulgate the information contained in Doc 10084, the SSCC will join with ICAO in developing and planning for regional workshops that will provide information and training on the contents of the new Doc 10084. The goal is to provide regulators, air navigation service providers and operators impacted by airspace disruptions with best practices and risk assessment strategies to mitigate these challenges.

Information on the SSCC can be found at the following: Safer Skies Consultative Committee (canada.ca)

In addition to the above efforts, IATA also participated in a short piece titled, "Assessing risk with imperfect information". The article underscores challenges faced by airlines in being able to access reliable information for threat and risk assessment activities. Source of the article can be located here: https://airlines.iata.org/issues/2023-issue-2

6.5 ICAO Security Week and IATA Security Forum

ICAO Security Week was hosted in Montreal, Canada between 23-27 October 2023. IATA was represented by nine staff and one advisor who participated on numerous panels as well as attending key sessions. In parallel of the ICAO Security Week, IATA organized its Security Forum (25-26 October 2023) with a joint Industry session on 25 October as part of the ICAO Industry Day. IATA promoted the ICAO Industry Day as a free-of-charge access and generated the participation of 85 participants.

During the session on *Flight Safety in Turbulent Times: Navigating Conflict Zones,* the IATA participant highlighted the need to provide operators with information related to both existing and evolving threats, as well as encouraged the utilization of the joint ICAO/IATA Contingency Coordination Team (CCT) concept. This concept has been widely used by several regions to mitigate airspace disruptions by rapidly sharing information between affected aviation stakeholders.

6.6 IATA Panel on Integrated Risk Management

As part of the Industry Day of the ICAO Security Week, IATA moderated a panel of experts to discuss Integrated Risk Management (IRM) as a systematic, proactive, and holistic approach to assessing and managing risk in any organization. In the context of civil aviation, it is widely known to involve the identification, assessment, and prioritization of potential hazards and risks, that lead to developing and implementing strategies to control and mitigate. The overall goal of the effort is to continuously improve the safety and security performance outcomes and organizational efficiency. The panel discussed the benefits of this approach towards a more informed decision-making process, a safer and more efficient operation, and evolve culture that values safety, security, and risk awareness.

The opening remarks by IATA'S Director for Aviation Security and Cyber highlighted:

- Advocating for IRM in civil aviation, emphasizing it as a method to improve safety, security, and resilience outcomes in the industry.
- IRM is seen to not only fulfil but strengthen promises made to passengers, crew, and stakeholders regarding safety and security, through a unified approach that learns from other sectors.
- The approach includes a broad scope of aviation security, extending beyond traditional measures to also cover aspects like cybersecurity and the impact of emerging technologies such as drones and AI.
- IRM can lead to more efficient resource allocation, ensuring that investments in safety and security have the maximum impact and help build public trust through transparency.

- Panel representatives were from Air Canada, Dragonfly Intelligence, FLYHT, Bank of Canada, and BGIS.

7 Security Management System (SeMS)

The main objective of that SeMS workshop conducted in the IATA Security Forum (2023) was to present some toolkits developed by a subgroup of the SeMS Aviation Community created as an outcome of the first SeMS Forum held in Madrid in November 2022. More than 70 professionals participated in both SeMS Workshop sessions, either in-person or online. The targeted audience involved the overall aviation ecosystem (and all entities beyond aviation) that could use such tools for assessing their own SeMS posture, based on the only Industry SeMS concept created in 2002 by the Global Aviation Security Action Group (GASAG) and then introduced as a mandate in the IOSA program in 2007.

Following the first SeMS Forum held in Madrid in November 2022, and comprehensive SeMS surveys conducted by IATA Security for response by all IOSA registered airlines clarified the magnitude of the current externalization of security operational functions.

The main outcome of the SeMS workshops (SeMS for ESPs and SeMS Strategy) conducted under the IATA Security Forum 2023 is the continuation of the finetuning of the developed SeMS for ESPs toolkit via a testing phase (from November 2023 to March 2024) regrouping more than thirty (30) participants from airlines, airports, external service providers, regulators, and security experts.

The proposed SeMS for ESPs toolkit shall then be shared within the SeMS Aviation Community when the ISM/17 will be published (April 2024) and advocated in the Regions as well as international forums such as the ICAO AVSEC Panel (35th meeting in April 2024). The proposed toolkit will also be included in the next editions of the IATA SeMS Manual and other relevant IATA Manuals, Documents and Programs as may fit.

IATA SeMS WORKSHOP / 2022

A risk-based and data-driven approach to security

'A Security Management System should be formulated through and incorporated within an organisations holistic Aviation Security Policy to generate maximum awareness, buy-in and real-world benefit across all levels of the organization'

8 Aviation Cybersecurity

Work on building a multi-year strategy within IOSA (IATA Operational Safety Audit) for Cybersecurity ISARPs (IOSA Standards and Recommended Practices) integration has been started. A detailed list of Foundational-ISARPs have been successfully identified by the cybersecurity team and they are now subject to further evaluation within the airline community. Once finalised and agreed the multi-year implementation phase will follow, hopefully within 2024.

In addition, during 2023, the IATA cybersecurity team produced two guidance material documents in respect of best practices in cybersecurity for Risk Assessment and Supply Chain Oversight. To enhance dissemination and awareness of the documents the IATA team hosted a webinar in June 2023. with support and contributions from airlines and IATA internal subject matter experts, which provided an overview of these new materials together with updates in respect of other IATA activities and initiatives within the cybersecurity sphere.

IATA held its 4th Session of its 3CTX (Cyber Threat eXchange) Open Forum (an invitation only event), under the theme of International Incident and Crisis Management. More than 35 participants including airlines, ANSPs (air navigation service providers), suppliers, OEMs (original equipment manufacturers), airports, academia, researchers, and other participants, exchanged thoughts and ideas on the challenges relative to the theme within a dynamic, constructive, and secure environment. Attendees also participated in an informative and engaging Table-Top-eXercise (the second of its kind), on the same theme. The exercise covered a variety of different malicious actions potentially posed by a bad actor to assist participants in further identifying, exploring, and discussing if, how and to what extent mitigation actions might be enhanced.

More generally the IATA Cybersecurity team is fully aware the international regulatory landscape is moving towards the creation and implementation of a variety of cybersecurity requirements for civil aviation. Regional entities are also increasingly introducing critical infrastructure regulations which the aviation industry will be subject to moving forward. Fully understanding and implementing a diverse set of regulatory requirements may be a struggle for international airlines, which is a critical reason underscoring why the IATA cybersecurity team continues to monitor, constructively engage with, and provide advice on a wide variety of cybersecurity documentation and requirements. There is a growing patchwork of regulations which many stakeholders will have to comply with in the years to come. As such the IATA Cybersecurity team will continue to play an active role in 2024 to assist industry in meeting those challenges.

One of those challenges, not unique to aviation, is in respect of the wider supply chain which, as for many other industries, is also a critical element when considering cybersecurity issues, potential vulnerabilities, and mitigation strategies. Existing technologies, as well as new ones, whether directly bound by civil aviation regulation or not, are potentially under threat on a regular basis. Given many security chains are only as strong as their weakest link it is of the upmost importance, more than ever, that supply chain elements are kept up to date and are segmented as much as possible, to restrict cyber-attacks as far as possible and limit potentially negative consequences to best effect.

8.1 International and Regional Regulatory Alignment

This table represents a high-level overview of the trajectory of regulatory evolution for aviation cyber security.

Key Standards Elements	ICAO A17*	UK CAA Cyber Assessment Framework	EASA Part-IS**	IATA CRMF
Identify critical information and assets	✓	✓	✓	✈
Assess the risk	✓	✓	✓	✈
Treat/transfer of risks and acceptance of residual risks	✓	✓	✓	✈
Monitor and adjust according to threat landscape	✓	✓	✓	✈
Response & Recovery from Incidents	✓	✓	✓	✈
Log & Report Critical Cyber Security Event		✓	✓	✈
Appoint responsible/accountable Senior Management Official		✓	✓	✈
Integrate in existing Safety Cyber Security Events in Management Systems			✓	✈
Maintain an Information Security Manual for airlines			✓	✈
Have the right people, with the right training and right resources	✓	✓	✓	✈

TABLE KEY

Covered by ICAO A17	**New**. not covered by ICAO A17	✈: Ed 1 IATA CRMF	✈: Ed 2 IATA CRMF	✈: Ed 3 IATA CRMF

* ICAO Standard 4.9.1[8] is introduced in the EU by way of Implementing Regulation (EU) 2019/1583.
** EASA Part-IS (implementing Reg - Feb 2026). Acceptable Means of Compliance AMC and Guidance Material GM are accessible here.

[8] Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

9 Air Cargo Security

9.1 TSA/EU Multilateral Summit

In February 2023, IATA hosted the Air Cargo Security Summit jointly organized by EU and TSA, with 49 airlines and 19 officials from 14 different Member States, including 18 participations from the European Commission and TSA combined. Participants exchanged perspectives, ideas, and updates on air cargo security requirements and operations within Europe. Officials from the TSA and the Mobility and Transport – European Commission provided industry stakeholders with an overview of air cargo security policy direction within TSA and DG MOVE.

As a result of the discussions, it was agreed to establish 5 working groups composed of regulators from both sides and the industry:

Scope of Working Group	Deliverables
Cargo Threat and Risk	○ Develop common language/terms on the topic of risk assessment. ○ Share respective risk methodologies to standardize risk factors and assessments. ○ How can carriers get compliance feedback (if it's not shared by the regulated entity)? ○ Request from the carriers to receive more information on threats (not at classified level) to understand the reasoning behind the requested measure.
National Civil Aviation Security Program Recognition (NCASP) & EU Air Cargo & Mail Carrier Operating into the European Union from a 3rd Country (ACC3)	○ Develop list of differences document, then work on improvements to include identifying opportunities for a global standard. ○ Green list of countries: work on those locations where discrepancies may exist/create a space for that exchange of information between the regulators (TSA, DG MOVE and EU MSs) and include industry. ○ Further work to be done in using the results of TSA activities in LPDs in ACC3 validations. ○ Seek avenues and synergies of using ACC3/RA3/KC3 validations in TSA activities.
Advanced Cargo Data	○ Improve communication with air carriers' when ACAS updates are made. ○ Harmonize data elements to develop a global standard. ○ Identify best practices for ensuring data quality. ○ More integration/harmonization of HRCM measures and allow time for implementation. ○ Interoperability of Pre-Loading /Advanced Information systems around the world through ICAO
Consignment Security Declaration (CSD)	○ TSA to identify differences to streamline the process in the Security Program(s) ○ Industry to support TSA in the assessment process.
e-Commerce	○ Establish a working group to determine what data is available and what are the gaps in the Security Program(s)

9.2 Consignment Security Declaration Workshop

In September 2023, IATA hosted a multi-stakeholder workshop in Geneva, supported by members of the CSWG and strategic partners. The workshop resulted in several key recommendations to improving the modernization and implementation of Resolution 651 on eCSD, as contained in the Cargo Services Conference Resolution Manual.

https://www.iata.org/en/programs/security/cargo-security/csd/

https://www.iata.org/en/publications/store/cargo-services-conference-resolution/

9.3 PLACI Implementation status

Back in 2019 the World Customs Organization (WCO) and ICAO jointly published guidance to that States could adopt where needed serving as an additional layer to support the management of air cargo security risk, in large part as a response to a variety of different security threats and previous incidents involving air cargo, in particular the events in 2010 often referred to as the "printer cartridge" or "Yemen plot". In this incident two improvised explosive devices (IEDs) were detected, following their departure from the point of origin (Yemen) on separate cargo planes that were manifested for the USA. This additional layer of cargo security primarily focussed on the timely submission to the relevant authorities of Pre-Loading Advance Cargo Information (PLACI) by airlines and freight forwarders.

PLACI requirements have been enforced in the USA since 2019 (previously ACAS – Air Cargo Advance Screening). In 2023 the EU, plus Norway (NO) and Switzerland (CH), started the implementation of their own PLACI requirements for all cargo and mail going to or through the EU/NO/CH territories. In addition, Canada, the United Arab Emirates and United Kingdom are all actively working on their own respective implementations which are expected to occur in 2024.

Such initiatives have a significant impact on air cargo operations and as such the IATA Cargo Border Management team maintains close communication with all relevant regulatory bodies and ensures, via active engagement and collaboration, that the industries views, recommendations, capabilities, and concerns are articulated, discussed and where possible considered.

Since July 2023 all airlines coming to or via EU/NO/CH must provide PLACI data to the relevant national customs authorities of EU/CH/NO before shipments are loaded at the last point of departure into those locations. Airlines and/or their respective cargo partners must also provide additional information/data, as directed within relevant aviation security regulations, prior to aircraft's arrival.

If at any point in the process a potential threat is suspected or indeed identified as the consequence of a PLACI risk assessment, a relevant notice is sent, by the relevant State authorities, to the airline or, if different, the PLACI filing party, seeking additional information, data, enhanced security screening and/or a notice that the cargo is not to be loaded onto the aircraft. Non-compliance for any PLACI filing can result in several different and escalating sanctions, which may include the cargo shipment being delayed up to and possibly including the suspension of the airlines' Operator Certificate in the case of repeated offenses/repeat offenders.

Full deployment of PLACI in all EU locations were expected to be achieved by October 2023, and penalties are expected to be applied and enforced from Q2 2024. The IATA Cargo Border Management team will remain keen observers of progress in all areas during 2024, paying specific attention to any operational difficulties that may arise and/or the identification and dissemination of suggested improvements, recommended best practices – providing constructive feedback to regulators, industry actors and other stakeholders as applicable.

Meanwhile, the IATA Cargo Border Management team is providing constant guidance to the industry through webinars, workshops, training (PLACI training) and a specific manual (PLACI Manual). In 2023 IATA Cargo hosted the annual IATA World Cargo Symposium (WCS), in Istanbul, Türkiye. The event ensured active engagement with a wide set of diverse aviation community members and the various regulators who govern much of what industry are required to do. The event was attended by 1250 delegates from all parts of the air cargo supply chain. This annual event will be hosted in 2024 in Hong Kong where IATA Cargo fully expects a wide variety of topical aviation security issues will be further articulated, discussed, and explored.

10 IATA Regional Security Overview

Owing to IATA's corporate structure, regional security efforts are vitally important import to delivery against global priorities. The specific regional make up can be accessed here - https://www.iata.org/en/about/worldwide/

10.1 Europe

Throughout 2023 IATA Europe has ensured they are closely engaged with and constructively contributing to several EC initiatives. For example, in early 2023, European Commissions Directorate General – Mobility and Transport (DG MOVE) started to develop a new AVSEC strategy to enhance and further educate how aviation security policies, regulations and concepts are better discussed, understood, and deployed in the future. Efforts to date have been primarily concentrated across three activity streams.

The first, the AVSEC baseline, looks to further explore potential improvements that may be generated following a carefully considered risk mapping exercise. This activity that highlighted several areas that may be suitable for enhancement, including within the detection and prevention capabilities of security equipment's deployed at airports. The DG MOVE working assumption is that benefits may be highlighted and adopted by the adoption of an outcome-based approach, an approach that would seek to evaluate security equipment as part of an overall holistic package of combined measures rather than seeking to evaluate individual security equipment's in isolation.

The second involves examining regulatory developments, to move away from a relatively complex body of rules, that may lead to discrepancies in implementation, and instead move towards an increasingly agile decision-making framework that would allow swift solutions to new and emerging threats, solutions and instructions that could be rapidly disseminated and incorporated. Such an approach would also allow emerging innovative technical solutions to be trialled and implemented in an increasingly timely, effective, and proportionate manner.

Such an approach links the third major stream of activity, the desire to establish an aviation security technology roadmap that allows regulators, industry and manufacturers to smoothly and effectively transition from the current technology position (equipment, layout, design and implementation) to any new and advanced future baseline that may be required in the years ahead, particularly in respect of aviation security equipment deployed for the primary screening of passengers, cabin and hold baggage.

IATA Europe has contributed to the US TSA (Transportation Security Administration)/ASAC (Aviation Security Advisory Committee) initiative, the ASAC international subcommittee that is specifically seeking inputs from non-US carriers particularly with respect to the Foreign Air Carrier Model Security Program. Such an approach, welcomed by industry, allows for a more strategic level of engagement e.g., regarding how security programs might look in the medium-longer term and how regulator/industry engagement might be improved moving forward.

In parallel IATA Regional Security European Focus Group is also exploring the current operational and economic impact of the existing measures and the degree to which these impacts may alter if/when existing mitigation measures and requirements are adjusted considering any review decisions that may arise.

Another key area where IATA Europe has taken a key interest concerns cybersecurity and the European Union Aviation Safety Agency (EASA), Part-IS regulation that will become applicable from 2026 to a wide range of stakeholders, including EASA-registered carriers, airports, and competent authorities. Part-IS aims to protect aviation safety against information security risks through the implementation of an Information Security

Management System, including both internal and external reporting schemes. This is considered one of the most advanced cyber regulatory developments so far, one that will be challenging for operators and authorities alike.

Looking ahead, IATA Europe seeks continuing areas for constructive engagement that will allow industry to educate, steer and support several key aviation security related projects and ongoing initiatives in an active, timely and constructive fashion.

10.2 Asia Pacific (ASPAC)

One of the strengths of IATA is its ability to reach, engage with and actively support a wide and diverse range of stakeholders, particularly within and across the aviation security arena. This is especially evident within the Asia Pacific (ASPAC) Region where IATA regional personnel can share global insights via regional events for localised consumption and potential adoption. This dynamic not only allows for a 'global down' approach to knowledge transfer but also enables an effective and timely 'local up' communication chain that better enables all parties with a vested interest in aviation security (local, regional, and global) to share information, ideas, recommended best practice and issues of concern. An approach that actively facilitates a shared understanding of the issues of today as well as the new and evolving challenges of tomorrow.

This collective and mutually supportive approach was particularly evident during the 11th ASPAC Regional Security Focus Group (RSFG) Meeting, held on the 18th of September 2023 during an in-person meeting in Hanoi, Vietnam. Participation comprised 31 representatives from 21 airlines with an operational presence in the ASPAC region, a region that encompasses 39 countries and where IATA currently has 47 member airlines. A region which is expected to lead global passenger growth over the next 20 years.

The event allowed IATA ASPAC representatives, and all attending the event, to share updates, discuss current activities and initiatives and agree future actions and deliverables. Of note were updates in respect of the work IATA had undertaken in respect of mapping cyber security regulatory requirements, those of ICAO and the extent to which these would impact regional operations and considerations.

IATA ASPAC also shared and collectively discussed if, how and to what extent it was possible to encourage and actively work with ICAO to ensure global aviation security guidance material could be enhanced and clarified to ensure universal understanding and adoption was improved.

The event also provided an opportunity for all participants to share, discuss and gain greater visibility of impending regulatory changes, challenges and/or opportunities across a variety of regional jurisdictions, including but not limited to; India, Japan, Australia, Indonesia, the Philippines and Vietnam, in addition to being briefed on non-regional updates, e.g., potential changes to European and/or USA regulatory requirements, for those carriers operating into those areas.

IATA ASPAC are looking forward to the challenges and opportunities that will no doubt arise in 2024, and the chance to engage in a dynamic, interactive, and informative set of debates once again at the 12th ASPAC Regional Security Focus Group Meeting.

10.3 Africa & Middle East

Throughout 2023, the IATA Africa & Middle East (AME) Operations, Safety and Security (OSS) office has been involved in numerous initiatives with stakeholders in the Middle East, North Africa, and Sub-Saharan Africa. In Q1 2023, AVSEC activities included supporting key influencer states such as the United Arab Emirates (UAE), Qatar, the Kingdom of Saudi Arabia, and Egypt in developing their security strategies and plans to enhance regulations. Additionally, in Q1 2023, while working with member airlines in Africa, IATA engaged regulators in

Kenya and the Kenyan Civil Aviation Authority to eliminate redundant, multiple screening processes, focusing instead on improving security and the passenger experience.

The AME team co-organized and led forums in both MENA and AFI for aviation security, notably with the African Civil Aviation Commission (AFCAC), Arab Civil Aviation Organization (ACAO), TSA Regional Industry Summits (RIS), and Airports Council International (ACI) Africa. These efforts aimed to promote a security culture, increase cooperation and information sharing among African Union (AU) member states, and showcase the potential benefits of One Stop Security (OSS). As a result, a few AFI states, most notably NBO Jomo Kenyatta International Airport, have since further engaged in OSS concepts.

IATA AME also conducted a Regional Security Focus Group meeting addressing key challenges in the AME region. These challenges included heightened geopolitical risks, conflict zones, deteriorating economic conditions, illegal migrant flows, human trafficking, and illicit trade and sanctions. Lessons learned included the constantly evolving risk mapping for members and the benefits of sharing information during critical events such as those in 2023 experienced in Sudan, Israel-Gaza, and Afghanistan.

The AME region experienced a range of geopolitical challenges throughout 2023, impacting member's aviation security, safety risk, and flight operations. Notable challenges included the fall of Sudan, ongoing security issues in Afghanistan, the Western Sahara dispute, conflicts in Somalia, Syria, Libya, Iraq, and Yemen. Since October, the region has grappled with the impact of the Israel-Gaza conflict, resulting in increased risk for IATA members, numerous flight cancellations, and heightened security measures at airports in the Middle East.

In collaboration with the US TSA, IATA AME co-hosted and organized the Africa Security Dialogue at IATA's Focus Africa event in Addis Ababa, Ethiopia, where TSA committed to partnering with IATA on improving security and capacity building for African states. Another initiative involved the US TSA Regional Industry Summit (RIS), in partnership with Emirates Airline and IATA, the Middle East Security Forum held in Dubai, U.A.E., with discussions focusing on flight operations from last points of departure from AME and the benefits of OSS as showcased by TSA.

The regional team was invited to be a member of the steering group for the ECAC-funded CASEII project for aviation security in Africa and the Middle East. Throughout 2023, there were two steering groups, with the third held in the Kingdom of Morocco, where IATA agreed to work closely with ACAO and AFCAC on a regional security roundtable for the following year.

IATA AME has also taken a keen interest in challenges and potential concerns related to cybersecurity. Throughout 2023, the region participated in two key working groups, one led by the Qatar CAA, and another by US TSA, which organized a cyber roundtable for AME stakeholders. Additionally, IATA supported the Republic of South Africa CAA with their regulations, including reviewing key areas of their cyber strategy, and supported the UAE with their policy.

10.4 North Asia

IATA's China and North Asia's (NASIA) regional headquarters is based in Beijing and serves as a central point for IATA's member airlines in the region. In addition to taking a keen interest in and being supportive of aviation security initiatives the regional office also conducts government and industry affairs in addition to preparing analysis and forecasting of developments in response to local policies and events.

The regional office has a wide and diverse area of operations and provides essential support services for the Northern Asia area which includes People's Republic of China (PRC); Hong Kong (SAR), China; Macao (SAR) China; Chinese Taipei; State of Mongolia; and Democratic People's Republic of Korea (DPRK).

During 2023 the NASIA security remained informed of a range of security updates, notably regarding Civil Aviation Administration of China (CAAC) regulatory changes to the 'National Civil Aviation Safety & Security Plan (2nd revision). This incorporated several amendments that stemmed primarily from ICAO (International Civil Aviation Authority) audits and wider changes to ICAO Annex 17. More notable aspects included 'clarification of roles and responsibilities', 'measures relating to off-airport checked-in baggage', and various updated commentaries regarding 'cybersecurity'. There were also updates regarding 'Civil Aviation Cargo and Mail Transport Security Rules' (2nd revision) which sought to bring mail into the aviation security regulations as well as some simplification of other procedures and formats.

In respect of passenger movements and facilitation, Border Control Authorities from Hong Kong SAR and Chinese Taipei have started the process of passenger's data exchange implementation (known as iAPI in Hong Kong, PNR in Chinese Taipei), to strengthen border control and public security.

One method the IATA NASIA office utilizes to good effect in ensuring messages and various updates are cascaded effectively is to conduct regional security workshops. One such regional security workshop was hosted in the IATA Beijing office on 28th November 2023. Main topics for discussion included Security Culture, SeMS and innovations in security practices. Approximately 60 representatives from a broad spectrum of organisations, including carriers, regulators, and other interested 3rd parties, attended the aviation security event where they were able to discuss and explore new information, regulatory requirements, and issues of concern in addition to sharing lessons learned, recommended best practice and new/emerging innovations.

One aspect the IATA NASIA office was able to update attendees on was in respect of IOSA security result analysis given it was now possible, with over 20 years of accumulated security data, to summarize findings from within the region, highlighting lessons learned, potential recommended best practice as well as identifying possible areas for further improvement.

As with many areas and regions, NASIA operators, across all aviation sectors, disciplines, and aspects, is not alone in having to face some common security challenges, including but not limited to difficulties associated with identifying and mitigating potential insider threats, real or perceived bomb threats and other security related incidents, particularly challenging when they occur upstream and emanate from outside the region and/or impact regional carriers and operations. These issues are not helped by growing geopolitical risks and several ongoing conflicts that have the potential to escalate. All of which are, in part, further exasperated by a lack of harmonization across different regulatory environments depending upon the different jurisdiction's carriers operate to and from.

All that aside IATA NASIA are looking forward to 2024, not least as they fully expect to maintain close working relationships with all relevant aviation security stakeholders in the region as they continue to assist all parties in better understanding and dealing with the many challenges faced by the aviation industry, not least in how to ensure security remains relevant, timely, effective, proportionate, and efficient.

10.5 Americas

IATA Americas has played an important role within and across the AVSEC community during 2023. Building upon some excellent initiatives and activities in 2022. IATA Americas has continued to actively support 'recognition of equivalence' (i.e. OSS) discussions during 2023 as many States, including but not limited to; Colombia, Peru, Brazil, Ecuador, and Bolivia, looked to explore if, how and to what extent OSS initiatives might be further progressed, agreed, trialled, and potentially implemented.

During 2023 IATA Americas actively supported 2 ICAO-led workshops specifically about OSS and recognition of equivalence. One workshop was delivered in Colombia in July 2023, with another being hosted at the IATA offices in Miami in September 2023. A commitment to continue discussing and supporting the OSS implementation was reached. It is hoped that these discussions and events will assist in helping all relevant parties to achieve a greater degree of mutual understanding, such that one or more initiatives may be further progressed in 2024.

Looking ahead IATA Americas will continue to provide coordination and communication facilitation, not least via the Americas Regional Focus Group, to ensure ICAO, State level actors, and other regional bodies and representatives remain aware of and consider industries concerns, priorities, and capabilities. IATA Americas regional and local representatives remain committed to ensuring communication channels remain open and that constructive dialogue and mutually beneficial information streams remain at the heart of all engagement.

Another avenue that IATA Americas utilized to good effect in 2023, to ensure industry views are captured and articulated in a timely and effective fashion, was via TSA/ASAC engagement in coordination with IATA Europe. IATA Americas is the co-chair the International Sub-Committee and coordinates a Working Group which better enables foreign (non-US) carriers to assist in providing direct feedback, in part via the creation of strategic recommendations, for TSA consideration.

IATA Americas also plays an important role within the ICAO Regional AVSECFAL (aviation security facilitation) Group which is also comprised of representatives from all States within North, Central, South America, and the Caribbean. IATA Americas actively engaged with this group at the last in-person meeting held in the Dominican Republic (June 2023), not least via the facilitation of a specific 'Industry Day' at the event and the creation and management of a dedicated Workshop on day 2 of the groups meeting. These IATA Americas-led opportunities allowed for much needed and wide-ranging debate, particularly on the industry side, regarding recognition of equivalence, baggage reconciliation and cyber security – in addition to facilitating informative discussions regarding the latest amendments to ICAO Annex 17.

Simulated emergency: real-life skills

Every emergency is unique. The best preparation is learning through experience.

IATA Training has added a real-time simulation feature to its Emergency Planning and Response courses for airlines and for airports and ground service providers.

Participants experience a simulated emergency, apply their knowledge, and judge their decisions in a safe and risk-free environment.

A dashboard displays the latest information. Incoming calls add to the realism while time is constantly monitored to ensure speedy decisions. Gather all the details and consult with your team for an effective, comprehensive response process.

Emergency response training has never been so realistic!

Request a demo for your team

For airlines
iata.org/training-talp04

For airports & GHSPs
iata.org/training-tapp12

IATA Training

11 Projects in 2024/2025

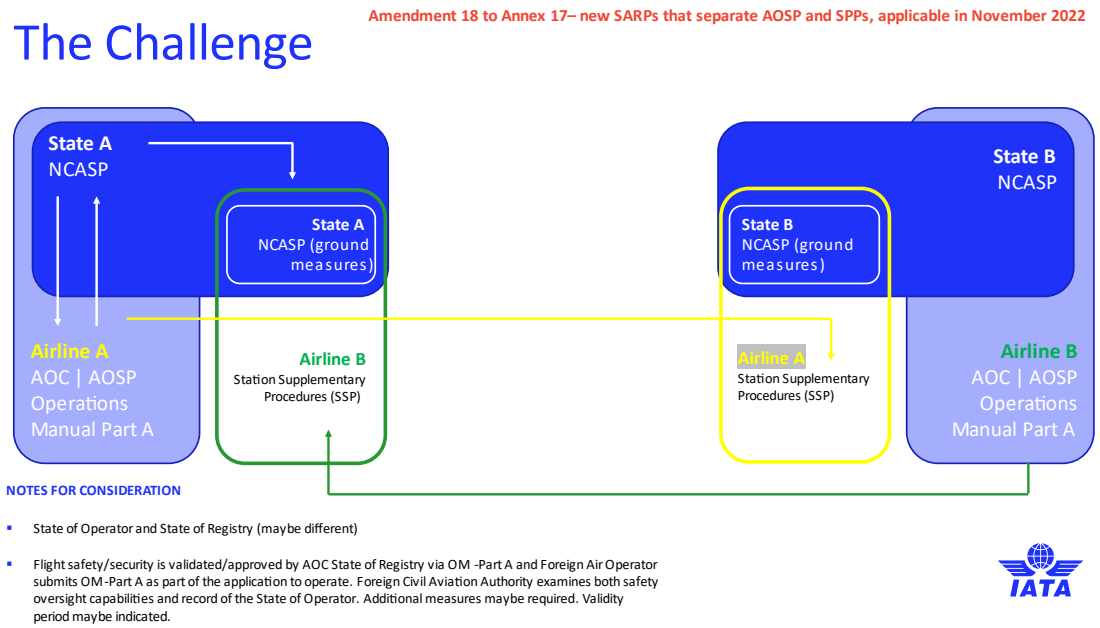
11.1 Aviation Security Trust Framework (ASTF)

Since the late 1970s, via ICAO Annex 17 obligations, aircraft operators have been mandated to create, submit, and secure approval for a comprehensive aircraft operator security program (AOSP) within their Air Operator's Certificate (AOC) jurisdiction, as well as for all foreign airports where they operate common carrier and/or charter services.

A primary obstacle to reforming this process has been focused on securing the exchange of security program information which has hindered the potential for new levels of collaboration and optimization of efforts. In this connection, IATA will spend 2024 developing the AOSP and related uses cases to leverage the concepts of "verifiable credentials[9]" that represents the opportunity to define secure information exchange and trust. The credentials are typically digital in nature and can include information such as identity attributes like qualifications, certifications, audit data or other relevant aviation security information.

More commonly, the key feature of verifiable credentials is the ability to be issued by one party (issuer), held by another party (holder), and presented to a third party (verifier) in a way that can be cryptographically verified. This verification process helps ensure the integrity and authenticity of the information being shared. The concept is part of efforts to create more secure, privacy-preserving, and user-centric approaches to digital identity and information sharing in aviation security.

There are several non-aviation security related use cases being developed throughout the civil aviation ecosystem that require future adoption and implementation. IATA is optimistically working on the notion that if the discipline of aviation security can demonstrate the highest levels of trust and integrity then it may prove a leading catalyst for wider ecosystem adoption and optimization.



[9] https://www.w3.org/TR/vc-data-model/

12 Products, Training, and Consultancy

12.1 Strategic Partnerships

Strategic Partners of IATA engage on aviation security and cyber security matters through collaborative efforts. These engagements typically involve sharing expertise, insights, and best practices to enhance global aviation security standards and information sharing. Strategic Partners often assist IATA to develop guidance and our member airlines in the implementation of security measures that address current and emerging threats in the aviation sector.

The below are active Strategic Partners who are acknowledged in this report as per the Strategic Partnership Program Terms and Conditions.

Securitas provides security solutions for airports, airport authorities, airlines, and other aviation-related businesses.

As a leading security provider, Securitas Aviation offers intelligent, integrated technology solutions adapted to a competitive and rapidly evolving industry.

We are a part of the technological advances as a catalyst for change, as innovative screening technologies, data analytics, automation and robotics become increasingly important, and as digitization enters the future ecosystems of our customers.

https://www.securitas.com/en/our-offerings/aviation-security/

MedAire, founded in 1985, has been the premier partner to the airline industry for health and safety solutions. MedAire combines global expertise and innovative technology to deliver comprehensive security solutions to clients. Our advanced portal offers a comprehensive library of aviation security reports in addition to real-time threat and incident monitoring, empowering aviation professionals to operate confidently and safely in a dynamic environment.

www.medaire.com

"We consider [Dragonfly's Security Intelligence & Analysis Service] SIAS to be a key enabling capability that contributes to our multi-layered threat monitoring program. The assessments are timely, reliable, and actionable. On a couple of occasions SIAS has provided useful early warning indicators for our operations, and therefore has provided situational awareness when we might not have known otherwise. We also regularly access their website for research purposes and that is particularly useful and user friendly. SIAS is a market leader and continues to evolve to suit client needs." As quoted by a Senior Aviation Security Manager from a major international airline.

https://dragonflyintelligence.com/

" LCB Worldwide has pioneered the Biosecurity at Border Crossings project during the Ebola Viruses Disease pandemic in West Africa. It was clear that Border Crossings and specially airports play a critical role in global connectivity, making robust preventive biosecurity measures paramount. Our Government and Operator Friendly Investment Model is the basis of our unwavering commitment to implementing state-of-the-art biosecurity solutions at airports, seaports and land border crossings which not only bolster the host country's defences against potential health threats while making sure that the project seamlessly integrate with the operational flow of the Airport facilities. LCB Worldwide's expertise in navigating the intricate landscape of biosecurity, coupled with our adherence to international standards, has significantly enhanced our confidence in ensuring the safety and well-being of travellers and international traders. LCB Worldwide is a proven trusted partner in the pursuit of elevated biosecurity standards for airports."

http://www.lcbworldwide.com/

Choosing Securiport for civil aviation security technology services has proven to be an invaluable investment for governments around the world. Securiport state-of-the-art solutions have not only streamlined security protocols but have also significantly fortified defense solutions against evolving threats in airports. The unparalleled expertise and reliability of Securiport makes the company an indispensable partner, ensuring the utmost safety of travellers' and integrity of airports infrastructure.

www.securiport.com

"Operating since 1998, FLYHT Aerospace Solutions Ltd. is headquartered in Calgary, Canada with offices in US and Germany. FLYHT has a global footprint with sales and installation support in China, Southeast Asia, the United States and Europe. We provide the airline industry with innovative data solutions to enable our partners to make smart decisions based on Actionable Intelligence to improve operational efficiency, sustainability, and profitability through our extensive hardware, software, weather sensors, and services.

In addition to Satcom solutions provided by the AFIRS 228™, FLYHT leads the charge in the 5G connectivity evolution with the industry-first AFIRS Edge™ WQAR solution to provide powerful situational awareness through real-time data, including an AID and Iridium Certus connection to flight deck EFBs. Our software solutions provide our partners with actionable intelligence that not only solves current problems but prepares them for the future in multiple areas, such as AHMS, Fuel and APU usage, Fleet and Turn management."

https://flyht.com/

Noem
Alha Airport MXP S.p.a
Collins Aerospace
ASM Security Management Company Limited
Beijing Zhongdun Anmin Analysis Technology Co., Ltd
CEIA S.p.A
Gozen Security Services Inc.
Nutech Company Limited
Orlando International Airport
Rapiscan Systems Pte Ltd
Securitas Transport Aviation Security
SITA

12.2 SeMS Manual, AHM, IRRM,

Part of the IATA SeMS Strategy is to ensure the continuous update and improvement of the IOSA Standards and Recommended Practices (ISARPs) in the Security Management discipline of the IOSA Standards Manual (ISM) with the IOSA Security Task Force (SEC TF see above paragraph 5.6), and to develop adequate guidance in different Manuals and publications. The audience is IATA members, but also IOSA registered airlines (not IATA members) as well as the broader aviation ecosystem will all entities involved in civil aviation supply chains, cargo operations, airport operations, and all potential external service providers for all operators.

The first publication directly linked to the SeMS Strategy is the SeMS Manual that could enhance company's security culture, regulatory collaboration and resource utilization as well as improve overall performance and communication within any organization. It contains security management guidelines on building effective aviation security measures and covers a range of additional topics including accountabilities and responsibilities assignment, risk assessment, security reporting and improved communication processes. The SeMS Manual has originally been designed for aircraft operators but is adjusted to any audience in the aviation ecosystem with any entities willing to translate the IATA SeMS concept into their operations.

A second important publication is the Airport Handling Manual (AHM) that is translating the "why shall we implement SeMS" into the "how" for ground operations. As mentioned in the SEC TF portion (para 5.6) and the SeMS portion (para 7), most of the IOSA registered airlines outsource their ground operational security functions to External Service Providers (ESPs) that are the main users of the AHM, and maybe not the SeMS Manual. IATA Core Security Department ensures coherence between the Standards contained in the ISM, the high-level principles contained in the SeMS Manual (the "why") and the more operational objectives in the implementation of all security measures on the ground (the "how") via AHM among other IATA publications.

A third important publication is the Integrated Risk and Resilience Management Manual (IRRM) that is designed to prepare to manage and react when "things go wrong". The Integrated Risk and Resilience Management Manual (IRRM) merges the previous Emergency Response Handbook (ERP) and the Integrated Risk Management Guide Manual (IRMGM), providing comprehensive guidance to any aviation entity who is planning to fully integrate their risk management components and improve their emergency capabilities. The IRRM showcases how to achieve full integration of any Safety Management System (SMS), Quality Management System (QMS), Security Management System (SeMS), Emergency Response etc., avoiding any risks associated with silos. The IRRM is situated above the SeMS Manual in terms of management perspective accompanying those entities willing to reach a "Leading" status in the integration of Safety, Security, Quality and Emergency Management Systems.

12.3 IATA Training

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 respectively the 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. Security training portfolio targets wide range of 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

2023 has been a year of restarting in security training, after recovery from covid impact. From smaller scale of virtual classrooms, evolved during the pandemic, we have started to see more return into classrooms and face to face training which has increased the training courses demand.

We have been conducting close to 80 various courses, with a balance of 75% face to face while 25% virtual training.

Training locations include our main training centres in Geneva, Singapore, Montreal, and Miami together with other smaller centres such as Amsterdam, London, and Milan. Public training in training centres or virtual classrooms, consist 80% of our trainings while the other 20% are delivery directly to clients as in house training (In-company)

The 5 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

The area of cyber security has gained momentum and over the last few years we have developed 3 courses that finally were clustered in 2023 as a diploma, which create high intertest in the industry and attract customers to this unique proposition.

IATA - Aviation Cyber Security Management Diploma

Together with our internal security team, we have continued the review on product content, keeping the quality and currency of content of our courses. We have been acceleration the active support of course deliveries by our colleagues from the security team which provide direct contribution to reaching our commercial target and generating revenue.

12.4 SeMS Certification

Growing interest is evident among industry participants in embracing a Security Management Systems (SeMS) approach to address risks in a more comprehensive and dynamic manner, extending beyond mere compliance with regulatory requirements.

To fully leverage the advantages of SeMS, these systems' practices and effectiveness can now undergo independent evaluation, certification, and widespread recognition.

IATA continues to invest in the concept of SeMS Certification in 2024, with foundational work having taken place throughout 2022 and 2023.

IATA, supported by various industry players including air carriers, ground handlers, and regulators, is working on developing tools to support further recognition of SeMS and for those operators who adopt and/or considering the approach.

Broadly, this involves a three-stage approach:

As part of the education component, IATA has created SeMS Community, and a quiz protocol, which is a free online tool designed to help individuals assess and demonstrate their understanding of SeMS, requiring a 90% pass mark. Furthermore, IATA is developing supporting materials to help those with a solid understanding of SeMS to gather evidence and evaluate the extent to which an organization understands and implements SeMS principles.

The materials and tools developed are agnostic and generic so that they can be recognized across different regulatory environments, jurisdictions, and sectors. The goal is for SeMS practitioners and adopting organizations to be able to document and present their security risk management and compliance activities in a detailed and evidence-supported way. To enable participants to showcase their security credentials both internally and externally.

The IATA strategy on this is driven by several factors, including the desire to demonstrate a security culture within an organization, manage risks more effectively, and reduce regulatory findings. Furthermore, SeMS adopting organizations aim to provide better data for Board-level decision-making regarding risk prioritization and mitigation strategies.

12.5 Consultancy

The Core IATA Security Team continue to assist IATA Consulting in designing and delivering on behalf of external commercial clients, competitive high-quality aviation security proposals and associated contracted deliverables. As one would imagine, aviation security consulting projects can and do range considerably in size, duration, value, and geographical location; but they are also increasingly supporting and engaging with a diverse range of non-aviation specific clients who are looking to leverage aviation security expertise and specialisms in areas that are not traditionally viewed as having AVSEC specific considerations.

IATA members continue to look to IATA Consulting for a range of supportive activities, not least in helping them to evaluate and redesign their Aircraft Operator Security Programmes (AOSP) and/or Supplementary Station Procedures (SSP). In addition, carriers, airports, cargo entities and others seek impartial support in respect of reviewing and adjusting their security culture posture and associated activities, evaluating, and assisting in the improvement of SeMS as well as conducting and reporting upon bespoke evidence-based gap and vulnerability assessments.

The IATA Security Team, working closely with IATA Consulting, have in 2023 actively supported, via both remote engagement and direct on-site delivery, consulting projects in Canada, South Africa, Mexico, Kenya, and Namibia while also offering advice, guidance, and support to prospective future clients as far apart as Azerbaijan, Nigeria, USA, Japan, and the UK.

Highlights in 2023 have included working collaboratively with a multi-national, multi-skilled team that is seeking to significantly disrupt and/or deter the illegal trafficking of wildlife, initially within aviation hold baggage and air cargo, via the creation, testing, operational trialling, and eventual wider adoption of new/innovative x-ray screening algorithms and associated operational protocols.

In addition, IATA Security Consulting is playing a crucial role in the security design of a brand-new international airport that is due to start operations late 2023/early 2024. Working in close collaboration with the immediate client, design and construction teams, technical experts, sub-contractors, and equipment providers/installers IATA is helping to ensure security considerations, design solutions and standard operating procedures are taking maximum advantage of internationally identified recommended best practice, lessons learned from previous similar contracts and the skills, knowledge, and in-house expertise of AVSEC subject matter experts.

It is a testament to the high degree of internal and external collaboration and support the IATA Security and IATA Security Consulting teams can consistently deliver to clients that many of the IATA Consulting contracts are in respect of multi-year projects, involving complex interlinked deliverables, large stakeholder groups and that some of these contracts, projects and deliverables are expected to continue into 2024 and beyond.

12.6 One ID Training & Publication

One ID is an IATA initiative that aims to streamline passenger journey with advance sharing of information and a contactless process at the airport based on biometric-enabled identification. From the aviation security perspective, One ID can bring the following benefits to the government:

1. Authority's direct control over which passengers are allowed to enter the country.
2. Opportunities to conduct a risk analysis on travellers through advance sharing of data and further combat cross-border criminal activities.
3. Prevention of document fraud and improved border security and passenger facilitation

IATA has been developing the One ID standards in collaboration with various industry partners and recently launched a new training course, One ID: Digital Identity and Biometrics Fundamentals, in order to provide guidance and support the industry in their implementation. Anyone who is interested in learning about the fundamentals of One ID is welcome to join the training. A publication, One ID Handbook, which will complement the One ID training, will also be available in early 2024.

13 2024 Forecast Statement

It's clear from a diverse group of internal and external participants that ensuring the safety and security of the civil aviation industry is defining. Activities, outcomes, personnel, communication, partnerships, and engagements between government and industry-wide stakeholders related to aviation security play a vital role in keeping employees and travellers safe.

It would appear equally true that the challenges the aviation industry and all those with a vested interest in protecting, maintaining, and growing it have faced in 2023, and will continue to face as we look ahead, are many and varied. It would also be fair to say that not all of them are directly regulated, or regulated in a timely, proportionate, harmonized, and cost-effective manner. Neither are the many and varied indirect threats that can and do significantly impact aviation operations, as opposed to those that directly target aviation specifically, being fully explored and widely discussed within international platforms with a view to, at the very least, ensuring they appear on risk registers.

We are increasingly conscious of the fact that industry actors and organisations, including State level regulatory bodies and international organizations, are seeking to work together to identify, agree, adopt, and implement systems, processes, technologies, requirements, and regulations that are, to a greater or lesser degree, mutually supportive, mutually recognised and, in some cases, mutually delivered.

As the size, scale, variety, and exposure of threats increase, not least those that are at times beyond the ability of individual industry stakeholders to influence or fully mitigate and/or that are in some circumstances not subject to direct aviation security regulation, the need to explore and adopt differing security postures and mitigation strategies grows. This is particularly clear when risks are driven or enhanced by geopolitical events far beyond the immediate boundaries of any single aviation environment or activity.

This can be equally true where technological advances may result in new and potentially unforeseen vulnerabilities. Yet ironically it is hoped these very advances in technical capabilities will also hold the key to increasing our security postures, efficiencies, and mitigation capabilities – enhanced capabilities that we anticipate will provide for a far more effective, secure, and user-friendly end to end journey. Scheduled and charter service jet propulsion is what we know today, but other alternative air services, using different device technologies may become, if we believe the value proposition, entirely customised to individual air travel needs. If so, we will need to be profoundly better in our risk-based implementation operations than we are today.

Some of the more pressing aspects, issues, and trends that IATA believes will be particularly influential and/or far reaching from an aviation security perspective in 2024 and beyond and which, as a result, will require a combination of careful and thought-provoking consideration, collaborative, and constructive engagement, mutually recognised and, where possible, harmonised mitigation strategies, are as follows:

Key Area	Description
Geopolitical risk and its interference with civil aviation	We appear, sadly, to be in a particularly turbulent period as far as geopolitical risk is concerned. The degree to which global events, be they currently known and with the potential to escalate beyond existing borders and boundaries, or unforeseen, with equally undesirable consequences, remains a real and growing concern. Especially so when seeking to determine, and potentially risk assess, if, how and to what extent local, regional, or indeed global air travel may be impacted. The more pressing and immediate issues that can and do arise as a result of geopolitical upheaval, e.g. temporary airspace restrictions, flight diversions, overflight considerations, cyber offensive disruption etc, are sub-risk elements that require consideration. However, it is equally possible that aviation generally, and individual aviation facilities, can also be targeted by those seeking to respond to and/or support (directly or indirectly) one cause or series of events. This could take the form of direct or indirect protests disrupting aviation operations, which may be violent or non-violent in nature e.g., the storming and occupation of critical infrastructure facilities, the blocking of access to facilities, breaches of perimeter security etc and/or could become far more violent and harmful e.g., deadly, and targeted acts of unlawful interference. As such, in addition to improving existing mitigation strategies via combination of physical, procedural, and technological mitigation we will also need, collectively, to become far smarter, effective, and targeted when considering how best to deploy time limited resources, threat and risk analysis, funding, assets and security personnel to best effect. IATA looks forward to supporting the delivery of the 2025 Safe Skies Forum edition with host State, Kenya.
SeMS – Security Management Systems	We continue to see real promise is in the continued evolution, understanding and wider adoption of SeMS. A growing number of regulators are increasingly looking to explore, support and promulgate SeMS as an effective and informed means of ensuring risks and compliance requirements are adequately managed in a timely, effective, and proportionate manner. IATA member airlines already adopt SeMS within their air carrier security programs and IATA continues to actively explore how and to what extent SeMS adopting organizations and SeMS practitioners can be more robustly supported, evidenced and if possibly, universally recognised by State regulators. Further work will be undertaken in 2024 and beyond for the extension of SeMS concept with External Service Providers (ESPs), SeMS Certification and it is hoped that SeMS will increasingly be adopted and widely recognised within the aviation ecosystem in the years ahead.

Risk based oversight and the use of data

A key element within any effective and timely SeMS approach is the use of incident and quality assurance data. As such the effective collection, retention, management, and assessment of data can play a critical role in how a SeMS approach to risk management moves forward in a predicative manner.

Threat assessment and risk management are key SeMS competencies. IATA has sought to progress and advocate for a greater use of open-source data when entities are looking to conduct near and medium-term horizon risk scanning, particularly when entities are looking to react to real-time scenarios and cannot (and should not) be solely reliant upon State level actors to provide direct regulation, advice, or guidance in real-time. The evaluation of real-time open-source materials, particularly where its identification, capture, timely transmission, and use can be actively facilitated by the growing utilisation of AI tools, needs to be more intelligently harnessed moving forward to support timely and effective risk assessment and SeMS related activities.

IATA and many regulators are increasingly of the view that effective SeMS practitioners, particularly those who can utilise and present data to evidence their security activities, risk management decisions and overall security deliverables will increasingly benefit from compliance and quality assurance regimes that seek to adopt and implement risk-based oversight strategies. Such an approach does not of itself generate or allow for reductions in direct regulation or standards, but rather seeks to ensure those who are less able to adequately document and evidence effective security mitigation and performance are subjected to increased oversight, thus ensuring limited resources are targeted to best effect.

IATA looks forward to supporting the delivery of the ICAO Security in 2024, with host State, Oman.

Passenger facilitation and the open architecture and other technological advances unlock

IATA recently endorsed the release of guidance by the Airports Council International (ACI) Europe, alongside various collaborators, on the implementation of open AI in airport security systems. Additionally, IATA released a Passenger Security Statement in 2022, supporting the adopting of these approach.

This endorsement aligns with the exponential growth in AI applications for aviation security, especially when integrated with open architecture across different security technologies and equipment manufacturers. This integration is expected to yield positive outcomes, enhancing the detection and performance levels for prohibited items, such as improvised explosive devices (IEDs). Automation not only presents an opportunity to improve the identification of traditionally challenging items but also aids in detecting and deterring items not presently considered prohibited in aviation security but are still significant for increased detection.

The use of innovative screening capabilities, combining AI and Open Architecture, in an interoperable manner, is anticipated to bring much-needed enhancements to the timely detection of a wide array of prohibited items, commonly referred to as "Automated Prohibited Items Detection Systems (APIDS). This includes traditional items like knives, as well as unconventional risks such as illegally trafficked wildlife and items of interest to state security. Beyond improving detection performance across various risk issues, this approach, with its automated precision, promises to elevate the passenger experience. It enables a more risk-based, differentiated approach to security checkpoints, enhancing the ability to detect and deter criminal activities within the aviation environment, going beyond conventional acts of unlawful interference.

The current technological trajectory offers a clear opportunity for advancing passenger facilitation and checkpoint performance. The growing SeMS community, increased use of data, adoption of AI, initiatives in open architecture, insights from the 2023 IATA Global Passenger Survey, and data from the IATA IDX depository collectively hold the potential for an effective combination. When aligned with outcome-focused regulation and risk-based oversight regimes, these factors can contribute to an increasingly automated, risk-focused, and user-friendly operational environment. This approach aims to deliver security measures that are proportionate, timely, effective, and responsive to the evolving threats on the horizon.

Emergency Response Plans (ERP) and Contingency Arrangements

The preceding discussion does not imply the absence of situations where unforeseen events may necessitate an emergency response, crisis, and resilience management planning, whether on an individual or collective basis. In such instances, it is preferable to have a well-thought-out and practiced emergency plan with established contingency and business continuity measures and approaches in place.

Although this report highlights the potential for entering a more unpredictable phase in terms of geopolitical events, there is an acknowledgment that, with our expanding capabilities, growing stakeholder networks, collaborative approaches, advanced technological insights, and a shared repository of lessons learned and recommended

best practices, one aspect that might become more predictable is our response and management of what is inherently unpredictable.

IATA looks forward to supporting the second ICAO Symposium on Assistance to Aircraft Accident Victims' and Their Families (AAAFV/2) in 2024, with host State, The Kingdom of the Netherlands.

Digital Evolution

Reflecting on 2023 and looking towards 2024 and beyond inevitably involves acknowledging the threats and potential opportunities that unfold within the realm of cyberspace. For those not deeply immersed in technical intricacies, distinguishing the extent to which 'cyber' is separate from various other technical aspects in our daily lives can be challenging. The prevalence of smart devices, notably our mobile phones, and the utilization of digital identities, digital handshakes, and biometric accreditations for online banking, and social media platforms are becoming increasingly familiar to us all.

The integration of artificial intelligence (AI) raises questions about its impact on our ability to use data safely and securely, both our own and with other entities. It prompts considerations on whether AI will enhance or undermine our trust in what we see, hear, and interact with. Exploring the potential of AI and other cyber-related tools, initiatives, and innovations in facilitating seamless border crossings, optimizing security controls, and designing effective risk-based solutions becomes paramount.

In contemplating the future, how AI, 'cyber,' metaverse realities, and digital advancements interact with and contribute to new aviation functionalities, especially in the security domain, remains uncertain. This includes aspects like single identity initiatives, the expanded use of autonomous vehicles, the deployment of innovative detection algorithms, and the evolution of passenger processing and risk assessment systems. Despite the questions that persist, the collective determination, collaboration, and will of the aviation security community inspire confidence that concerted efforts will be made to collaboratively address the challenges that lie ahead.

With the continuing development of the "connected aircraft", many organizations in the digital supply chain face the potential to be targeted by cyber threat actors not just for their Intellectual Property and proprietary information, but because the supplier's products may provide these threat actors access to the digital systems of an airline customer.

This phenomenon – where a supplier inherits the security risk profile of their customer – is not new to aviation security. Contracted air supply, cargo, and ground-handling companies have long-been identified as potential threat vectors to commercial flight operations and are subject to compliance with airline operator security programs.

In addition to developing cybersecurity standards to be incorporated into aircraft operator security programs, FLYHT advocates mitigating this "inherited risk" in the digital supply chain by engaging in close collaboration with airline customers to identify mutual threats, develop wholistic risk profiles that account for integrated technological systems, share intelligence, assess vulnerabilities, and implement coordinated mitigation measures – both proactively and in real-time – that minimize impacts and ensure timely and cost-effective recovery to incidents.

FLYHT's participation in IATA's Aviation Cyber Security Strategic Partnership is integral to this endeavour."

In summary, 2023 marked another year of significant progress.

This progress was evident in the industry's ongoing recovery from the global pandemic, demonstrating resilience in adapting to heightened demand and the resulting pressures on facilities, equipment, and personnel. Moreover, advancements were observed in the collaborative efforts of diverse stakeholders committed to upholding aviation as the safest and most secure mode of transportation. These stakeholders actively engaged in enhancing the operational environment, encompassing physical, technical, and regulatory aspects, to collectively enhance our capacity to provide effective, timely, proportionate, and pragmatic security in a sustainable and risk-based manner.

Looking ahead, optimism for 2024 stems from the belief that combined endeavours will yield even greater innovation and improved security performance and outcomes.