POSITION PAPER

Security Management Systems (SeMS) Policy

Strengthening Aviation Security through Risk-Based Security Management

Summary

Civil aviation security rests on a regulatory framework that States establish through ICAO Annex 17, National Civil Aviation Security Programs (NCASPs) and oversight. That framework sets the baseline and will continue to do so.

The global rule base approach has grown steadily for two decades while measured implementation has plateaued. More prescriptive measures no longer are converted into more security. The binding constraint is not the number of standards or national regulatory requirements but the capacity of organizations to manage security risk against them.

A Security Management System (SeMS) is the mechanism that closes that gap. It does not replace the mandated baseline. It holds the baseline and the risk-based measures that go beyond it so that both answer to a single accountable security outcome and so that assurance evidence feeds back into how oversight is targeted towards where the risk is needed to be mitigated

IATA does not seek an international standard and/or regulatory mandates for SeMS. The mandated baseline of ICAO Annex 17 applies to States and all operators and should stay that way.

IATA believes that operators that have voluntarily implemented a robust Security Management System (SeMS) should be recognised by States for doing so. This may apply to airport operators and other stakeholders or via IATA's own mandatory requirement for IOSA registered airlines, including IATA member airlines.

Where an operator can demonstrate that its SeMS effectively manages compliance, risk, and assurance to a recognised standard, the State should take this into account in its oversight approach.

This recognition should lead to a different relationship between the State and the operator. It should influence how the operator is overseen, the level of trust placed in the operator's own assurance processes, and the extent to which the operator is involved in discussions before regulatory or operational decisions are made.

SeMS is a route open to any operator; the benefits should accrue to those who take it.

IATA's position is thus:

1) IOSA-registered airlines, including IATA member airlines, have been required to implement a Security Management System (SeMS) since 2007. Compliance is independently audited every two years through the IOSA program and remains a condition of IATA membership.

   IOSA evaluates how effectively airlines have implemented SeMS, including their Aircraft Operator Security Programme (AOSP). This programme incorporates the security requirements of both the airline's home State (core AOSP) and the States where it operates (SSPs when necessary).

   IATA is not seeking to make SeMS mandatory across the entire regulated aviation system. For many entities, existing regulatory requirements remain appropriate.

   Instead, IATA is asking States to recognize the commitment airlines have already made through the IOSA program. States should also extend similar recognition to any operator that voluntarily achieves a comparable level of security management, with appropriate benefits and recognition for those that do so.

2) States should recognize operators that achieve a defined SeMS maturity level, through their own assessment or acceptance of an independent one and reflect that recognition in how those operators are regulated and overseen. This can be reflected in the trust placed in the operator's own assurance, in the frequency, depth and scope of oversight, and in the acceptance of the operator's assurance of its contracted service providers as part of its oversight strategy.

3) Recognized operators should be brought into pre-decisional consultation on evolving regulatory policy and on time-sensitive threat-based measures, so that their risk and performance evidence informs what is proposed, and so that measures are proportionate, feasible and implemented in a coordinated, risk-based manner.

4) Aviation security policy should adopt security outcome equivalence as a governing principle. Regulated entities should be held to equivalent security outcomes, not to uniformity of means. Where a recognized operator has, through its own risk assessment, adopted measures beyond the mandated baseline or an alternative means of achieving a prescribed outcome, States should assess those operator own measures on their demonstrated effectiveness, accept them where the outcome is equivalent, and take them into account in determining the operator's oversight and any additional measures required of it.

5) Oversight of recognized operators should be risk based and performance based, informed by SeMS generated evidence and common security performance indicators, with proportionate treatment of findings and protection of the information that operators share.

6) A common SeMS maturity model, with defined and evidenced levels, should be agreed between industry and regulators as the basis for recognition. Recognition is earned and maintained. Then it is subject to review and can be withdrawn.

7) Recognition and assessment results should be portable across authorities, supported by digital trust so that evidence can be verified across organizational and national boundaries without repeated assessment.

8) SeMS should be integrated with safety, information security and quality management rather than operated as a separate system, and regulators should accept integrated arrangements to meet the requirements of each domain.

9) ICAO should continue to strengthen the security management related provisions of Annex 17 and guidance in Doc 8973 and support their promotion and implementation across every tier of the security chain, including External Service Providers (ESPs).

What is SeMS?

A SeMS is a structured, organization wide framework for managing security risk.

It comprises four interdependent components,

- security policy and governance, including an accountable executive, defined responsibilities and resourcing,
- security risk management, through threat and vulnerability assessment and the selection of proportionate measures;
- security assurance, through monitoring, audit, performance indicators, management review and corrective action; and
- security promotion, through training, communication and culture.

The key concepts of security management already sit within Annex 17 provisions and the guidance contained in the ICAO Aviation Security Manual (Doc 8973, Restricted).

For aircraft operators, who are IATA Members or IOSA registered members, SeMS has been a binding IOSA standard since 2007, and was extended in 2024 to address security management by ESPs.

ACI World has promoted similar concepts for airports operators, the UK Civil Aviation Authority has published their own SeMS framework, and several states are evaluating SeMS conceptually.

SeMS is therefore not a new idea or an industry alternative to regulations. It is the implementation discipline that turns a standard into something an organization can run efficiently, evidence and improve.

SeMS enhances the regulatory framework

Regulation establishes what must be achieved and provides consistency and accountability across the global system. Compliance with the baseline is inherited down the chain from ICAO Annex 17 to regional and national rules, to the operator's program and to the ESPs who, in the case of aircraft operators, implement the bulk of ground measures on the operator's behalf.

What regulation does not do is tell an organization how to achieve those outcomes within its own operating environment, or how to know whether they are being continuously achieved between oversight inspections for example. SeMS provides the governance, risk management, reporting and assurance practices through which an organization continuously evaluates its own performance and adjusts. Rule and risk sit inside one structure. The result is an overall system that remains compliant while becoming more responsive to emerging threats, operational realities and changing priorities, and in which each tier can verify the tier below it with a depth set by risk rather than by the calendar.

Adaptability in a dynamic threat environment

The threat environment changes continuously through geopolitical developments, technological change, evolving attack methods, insiders and newly discovered vulnerabilities. Regulatory processes must, properly, pass through consultation, legal review and implementation periods, and so cannot always move at the pace of operational risk that operators ultimately face.

SeMS provides the mechanism for ongoing risk assessment, monitoring and adaptation.

An organization with a functioning SeMS identifies changes in its environment, assesses their impact and implements proportionate responses before risks materialize into incidents, rather than after deficiencies are found by inspection or exposed by events.

It does not create a separate security system. It keeps the mandated measures relevant and effective between regulatory oversight cycles while preserving alignment with national and international requirements.

Security Outcome Equivalence (OSS version 2.0)

Airlines, airports, ground handlers, cargo and catering providers and air navigation service providers face different threat levels, resources, business models and operational complexity. The same security challenge may require a different mitigation depending on who is implementing it and where. A measure that is effective in one environment may be unnecessary, impractical or less effective in another.

Aviation security policy should therefore focus on achieving equivalent security outcomes rather than enforcing uniformity in the means used to achieve them. SeMS gives organizations the process to evaluate risk, identify root causes and implement solutions aligned with the required outcome, and gives regulators the evidence to accept those solutions.

This is what allows innovation and flexibility without weakening standards, and it is what makes proportionality possible. A small operator or a single-site service provider can run a SeMS scaled to its risk and size, with the same components and the same accountability as a global carrier.

Outcome equivalence is also the principle on which recognition arrangements between States, such as One-Stop Security (OSS), depend. IATA considers it a key principle for future aviation security policy development.

Oversight Maturity

Regulators are increasingly pursuing risk based and performance-based oversight models that direct resources to where risk and impact are greatest. Such models require reliable information on organizational risk, vulnerabilities, performance and mitigation. SeMS generates exactly that information. Formal risk assessments, assurance results, internal reporting, management reviews and Security Performance Indicators (SePIs) that together give a far richer picture than a checklist inspection can.

SeMS is therefore a force multiplier for oversight.

Regulators gain visibility of operational security performance without a proportional increase in inspection resources, and organizations become active participants in finding and fixing vulnerabilities.

Two conditions apply.

First, common SePIs are needed so that performance can be compared and benchmarked meaningfully across entities and States.

Second, the information that entities share must be protected. Used for oversight and improvement, not as a source of penalty for the organization that reported it. The just-culture principles that made safety reporting work apply equally to security.

Outcome equivalence and risk-based oversight only function if a regulator can tell how mature an organization's SeMS is. Industry and regulators should therefore agree to a common SeMS maturity model with defined levels, for example present, suitable, operating and effective, and a bounded set of objective evidence for each.

The definition of the operating level matters because it is the point at which an organization can be said to be managing security rather than documenting it.

IATA's SeMS Certification Program (SeMS CP) provides an independent, standardized assessment against such levels. Its value depends on recognition. An assessment result accepted by one authority should not have to be re-established by the next. Authorities should apply proportionality in categorizing findings at each maturity level, calibrate their assessments centrally, and provide an advisory route for resolving disagreements over qualitative criteria before enforcement.

Recognition in turn depends on evidence that can be trusted across boundaries. Today the verification of a program approval, a certification status or an audit result between a State and an operator, or between an operator and a service provider in another jurisdiction, runs on assertion, paper and repeat audit.

Digital trust, as demonstrated by the Aviation Security Trust Framework for AOSP and SSP cycles, allows a verifier to confirm that an attestation is genuine, current and bound to a specific document without any bilateral integration.

Applied to SeMS certification and, further out, to OSS decisions and assessor credentials, it is what makes risk-based oversight of a distributed supply chain defensible rather than aspirational.

Integrated Management Systems

Regulated entities are increasingly expected to operate a safety management system, an information security management system and quality or compliance monitoring functions alongside security. Where these are run as separate silos, the result is duplicated governance, fragmented risk pictures and competing demands on the same accountable executive.

SeMS should be designed and recognized as one leg of an integrated management system. Security, safety and information security risks should be assessed within a shared framework, reported through common channels and reviewed together at management level, with a single view of the interdependencies between them: a cyber compromise of an operational system is a security event with safety consequences. Regulators should accept integrated arrangements as meeting the requirements of each domain and should coordinate their own oversight of them accordingly.

Conclusion

Decades of rulemaking have produced a comprehensive baseline for aviation security, and it should remain the foundation. The next gains of security and efficiency will not come from adding to it. They will come from the capacity of organizations to manage security risk against it, and from oversight that recognizes demonstrated capability rather than documented compliance.

IATA does not ask States to mandate SeMS. The airline sector has already made that commitment through IOSA two decades ago and verifies it on every registration cycle for aircraft operators. IATA is also offering an independent assessment of the SeMS maturity of all operators and stakeholders interested in via its SeMS Certification Program (SeMS CP).

What IATA asks is that States make use of it. Recognize operators that reach a defined level of maturity, place proportionate trust in their own assurance and in their oversight of the External Service Providers (ESPs) who deliver on their behalf and bring them into the room before regulatory policy and time-sensitive measures are decided.

Where an operator's own measures achieve an equivalent outcome, that equivalence should be accepted, and ideally recognition of equivalence granted by one mature authority should extend across borders. It is also the only realistic route to oversight that concentrates resources where risk is greatest, to a supply chain that can be verified rather than asserted, and to a system that adapts at the pace of the threats it faces.