Security Incident Reporting

Legal Background

As mandated by **ICAO Annex 17** – *Aviation Security*, States must:

1. Ensure that their national civil aviation security programme defines processes for the reporting of information concerning incidents of acts of unlawful interference and preparatory acts thereto, by any entity responsible for the implementation of the National Civil Aviation Security Programme (NCASP) in a practical and timely manner to the relevant authorities (**Standard 5.1.6**); and

2. Ensure their National Civil Aviation Security Quality Control Programme (NCASQCP) includes, *inter alia*, a confidential reporting system for analyzing security information provided by sources such as passengers, crew and ground personnel (**Standard 3.5.1 d**) and any other person in the aviation sector.

Accordingly, as mandated by the **IATA Operational Safety Audit (IOSA) Standards Manual (ISM)**, Airlines must:

1. Implement an operational security reporting system throughout the organization in a manner that:
    a. Encourages and facilitates personnel to report security incidents and security occurrences pertaining to the Operator;
    b. Ensures mandatory reporting in accordance with applicable regulations; and
    c. Includes analysis and management action as necessary to address security issues identified through the reporting system. (**ISM SEC 1.12.1, ISM/17, 2025**)

2. Have a process that ensures notification to the applicable aviation security authorities when a reportable security incident, including serious incident that may lead to an act, or an attempted act of unlawful interference, has been identified (**ISM SEC 4.3.2, ISM/17 adjusted in ISM/18, 2026**)

To assist stakeholders, in June 2022, ICAO with active involvement from industry, developed guidance material on the implementation of a reporting system, and established a common taxonomy, in an effort to structure and harmonize the reporting process of aviation security occurrences and incidents. The ICAO Incident Reporting Guidance and Taxonomy is a public document available in the six (6) ICAO languages. The ICAO guidance material is fully aligned with the IATA harmonized security taxonomy promoted in the SeMS program and the SeMS Manual, as well as the IATA Incident Data eXchange (IDX) safety and security incident data management program.

With the incremental level of outsourcing in the aviation ecosystem, and Annex 17 Standard 3.5.3 obligation for each entity responsible for the implementation of relevant elements of the NCASP (thus Operators) to periodically verify implementation of security measures outsourced to External Service Providers (ESPs) complies with the entity's security programme. Note the Operator (first party of the outsourcing) remains the entity responsible for the implementation performed by its ESPs (second parties of the outsourcing, see definitions).

Furthermore, the scope, magnitude and accountability linked to the reporting of security occurrences and incidents between ESPs and Operators, and then between Operators and Authorities, should be fully harmonized and globally implemented. It should also be acknowledged that only entities mature in aviation security, or having deployed a Security Management System (SeMS), could perform adequate threat assessment of reported occurrences, and then appropriately decide which occurrences be elevated to reportable incidents.

Definitions

Security Occurrence: Any security-related event that may result in a reduced security outcome, potentially increases operational risks or endangers the safety of passengers, crew, ground personnel and the general public, or potential non-compliance. This includes the identification or observation of a vulnerability in the protection of civil aviation against acts of unlawful interference. (ICAO Doc 8973, and public Incident Reporting Guidance, 2022)

Security Information: Could be included in the definition of security occurrence when the "event" is an "information" worth reporting. [IATA, new]

- *The ICAO guidance goes further in explaining that events [or information] and activities that appear to be abnormal, unusual, strange, etc. should be reported internally or directly to authorities through appropriate channels by any person. This is the example of a witness informing airport staff or the police about the piece of luggage left unaccompanied in public area. This could also be the case of an access door kept open when it should be securely closed. If that observation, impression, feeling, or activity is not reported, then it is lost even if it could have been a good indicator or precursor for security analysts*.

Security Incident: A designation given to a security occurrence which affects or could affect the safety of passengers, crew, ground personnel and the general public. Security incidents are designated by a security official or manager to a reported security occurrence based on an analysis of the occurrence and a determination that additional action is required. (ICAO Doc 8973, and public Incident Reporting Guidance, 2022)

- *Security incidents are security occurrences reported by staff, crew, ground personnel, subcontractors, media, the public and/or passengers that are analyzed by a security subject matter expert, for example the security official or manager of the entity who received report, or the authorities in case of direct reporting. A security incident is potentially threatening and could lead to harming the public, staff, and/or crew, to disruption of service, to loss of reputation, and should always be taken seriously*.

Serious Security Incident: A designation of an incident in case of which the risk assessment indicates high probability of escalation to an accident as the most credible scenario, or with serious and immediate impacts on the level of aviation security, and in case of which there are no or only limited or insufficient preventive measures remaining to avoid the accident, or the accident was avoided only due to coincidence, or pure luck. (IATA SeMS Manual, 2025)

- *The definition of serious security incident derives from the definition of "serious incident" contained in ICAO Annex 13 – Aircraft Accident and Incident Investigation, as the difference between safety and security could only be clarified in the end of the investigation.*
- *In this definition, the term "accident" should be understood as defined in ICAO Annex 13 which mean the final determination of an accident as an act of unlawful interference will be the matter of further investigation identifying if the accident happened due to any malicious intent.*

Act of unlawful interference: A serious security incident that a State decides to officially report to ICAO according to Annex 17 Standard 5.3.1 and following the model of "official report on act of unlawful interference" as contained in the Appendix 42 to the ICAO Aviation Security Manual (Doc 8973, 2022, Restricted). [IATA, new]

- *Annex 17 defines various events (acts) as acts of unlawful interference. Acts of unlawful interference are also defined in Article 1 of the different ICAO Conventions and Protocols (Tokyo, 1963, The Hague, 1970, Montreal, 1971, Montreal, 1988 and Beijing, 2010) as ratified and adopted by States.*
- *Therefore, the definition of acts of unlawful interference (including specific acts) varies between States, as determined by their respective NCASP.*

Report Originator: Legal entity or person who reports a security occurrence on a voluntary basis, or a security official or manager who analyses occurrences, qualifies them as incidents, and reports them internally (for resolution) and externally to other entities (Operators for ESPs) and authorities (when mandated). [IATA, new]

Outsourced Operational Functions: Where an operator has chosen to outsource operational functions specified in IOSA provisions to External Service Providers (ESPs), conformity with those provisions will be based on evidence provided by the operator that demonstrates acceptable processes are in place (i.e. processes that are documented and implemented) for monitoring such external service providers to ensure fulfillment of applicable operator and regulatory requirements affecting the safety and security of operations. Auditing is recommended as an effective method for an operator to monitor external service providers. (ISM/17, 2025)

Outsourcing: The business practice whereby one party (e.g. an operator or provider) transfers, usually under the terms of a contract or binding agreement, the conduct of an operational function to a second party (e.g. an External Service Provider, ESP). Under outsourcing, the first party retains responsibility for the output or results of the operational function even though it is conducted by the second party. (IRM/14, 2025)

- Note that the entities responsible for the implementation of the NCASP according to ICAO Annex 17, that are outsourcing operational security functions to External Service Providers (ESPs) remain fully responsible for the output or results, or implementation of all the measures that have been outsourced, as well as for the quality control and quality assurance functions and oversight over their ESPs.
- The ESPs may also be recognized as separate entities responsible for the implementation of the NCASP according to ICAO Annex 17 when they are specifically mentioned in the NCASP as responsible for some specific measures, not as service providers for an operator or other entity also responsible for the implementation of the NCASP.

General Objectives of Security Incident Reporting

As already mentioned, the incremental level of outsourcing in the aviation ecosystem could potentially dilute the responsibilities for when and how occurrences and incidents should be reported, either between External Service Providers (ESPs) and Operators, or between Operators and Authorities.

General facts about incident reporting should be structured as follows (see Figure 1 – Security Reporting Process Flow for more details):

1. Security occurrences could be reported by anyone, public, internal staff, crew, external staff, using incident reporting forms, platforms or websites developed by operators and/or entities,
2. Security occurrences should be sent (preferable immediately) to the security departments of the entities directly concerned so that they could assess the potential vulnerabilities and threats,
3. Security occurrences reported by External Service Provider (ESPs) staff should be shared with the security department of the Operators concerned (ESPs clients) for further analysis,
4. Security occurrences must only be analysed by a security official, or manager designated by the ESP or the Operator as part of the SeMS implementation,
5. Only recognized security official or manager from SeMS entities (ESPs or Operators) should be in the position to elevate a security occurrence to a reportable security incident,
6. Security officials and managers should always follow the official security taxonomies developed by ICAO (public guidance material) and/or IATA (IDX) for harmonization, sharing and analysis purposes,
7. Information contained in security reports shall be protected as sensitive aviation security information,
8. Mandatory reporting of security incidents to authorities must be performed by security official and manager personnel of SeMS entities (Operators and/or ESPs) only, for consistency purposes,
9. IATA has developed short videos on security awareness and security reporting available on IATA SeMS page (YouTube), and on the SeMS Aviation Community (high quality).

Additional Remarks

Risk analysis, usually the responsibility of the Security department of a SeMS entity (Operator or ESP), should be recorded, preferably in a standardized manner, for methodological consistency and trend analysis. Security risk assessment should also prescribe the authority level required to authorize continued operation at that risk level without mitigation. If the risk assessment reaches an established tolerability threshold, related to an entity's risk "appetite", appropriate mitigations should be proposed and agreed upon so the risk could be decreased to an acceptable level.

When mitigations include undertaking certain actions, responsibilities and deadlines should be clearly established and assigned to ensure effective implementation. As part of a follow-up assessment, an entity should establish a timeframe for examination of implemented actions to reasonably ensure desired effects were achieved and unintended consequences avoided or adequately identified.

To encourage a **positive security culture**, entities should empower frontline staff. Entities concerned should dedicate sufficient time for thorough and targeted analysis and reaction.

Finally, Authorities informed about an incident should refrain from undertaking any regulatory actions or issuing findings in a purely regulatory or punitive manner. This is also highlighted in the ICAO guidance as one of key principles of developing a healthy security reporting system and overall security culture.

IATA SeMS Manual (2025)

Security Reporting Process Flow

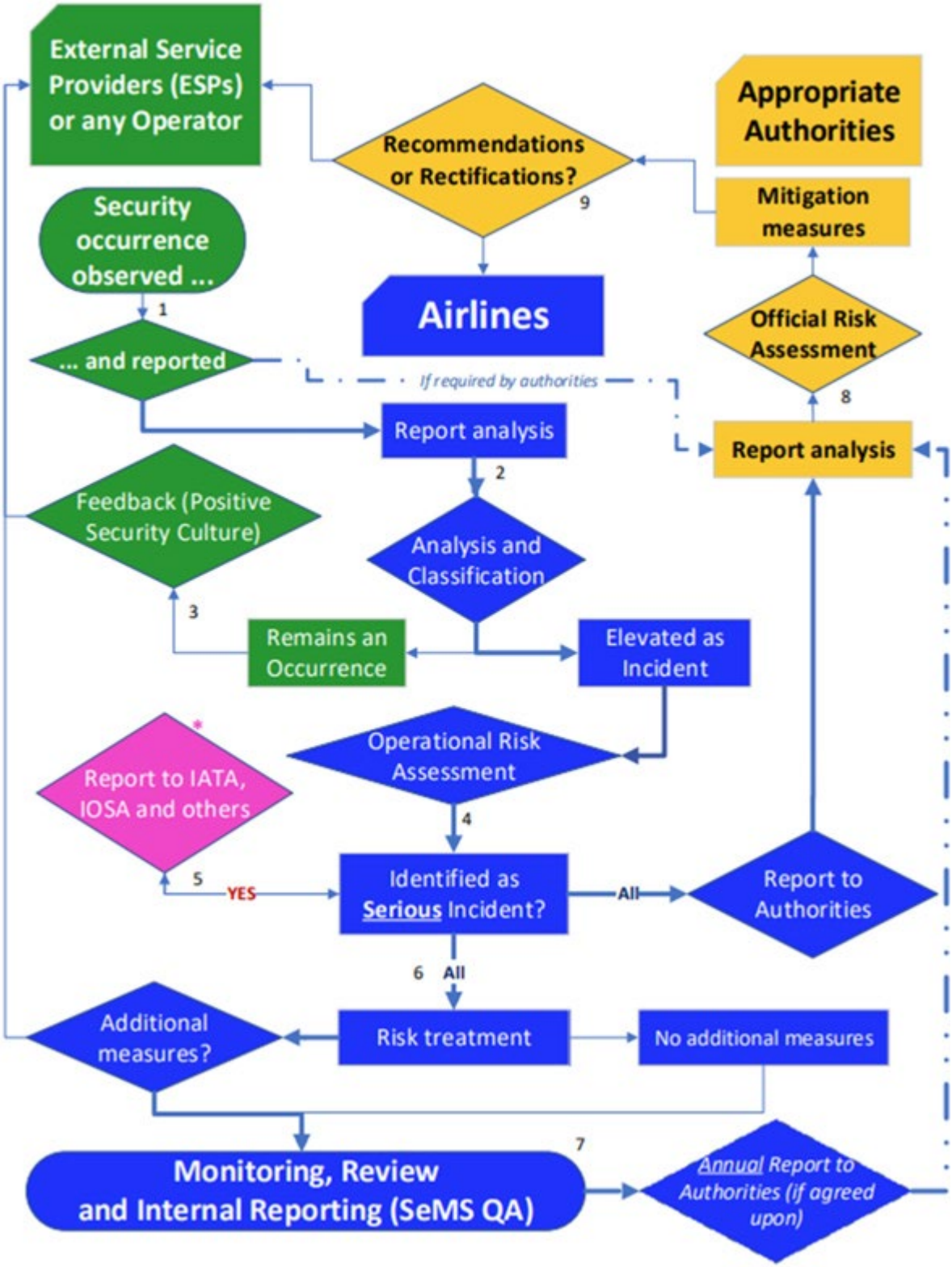

Figure 1 - Security Reporting Process Flow
Source: IATA

Figure 1 - *Security Reporting Process Flow* describes the process flow starting from the source of occurrence (step 1) and finishing by potential recommendations and/or request of rectification by the authorities (step 9). It describes interdependencies between three generic entities: an External Service Provider (ESP) or any other operator, the airline and the Appropriate Authority.

Following steps take place in the process:

1. Security occurrence is identified (by any member of personnel) and the report prepared by the authorized person from the ESP (or other operator) organization is submitted to the air operator (airline). In some jurisdictions reporting to the Appropriate Authority may be also required directly from the ESPs. ESPs should however conduct their own risk assessment (as part of their SeMS) which considers information based on reported occurrence.

2. The report analysis and classification are performed by the airline. Submitted reports would typically be first subject to an initial review and analysis to assess their validity. It is understandable, assigning the occurrence to a specific category (of taxonomy) requires certain security expertise therefore it is not required by the ESP (in step 1) when submitting the initial occurrence report. Classification should occur once the report is analysed and will include assigning the taxonomy category and deciding if the event remains as the occurrence or is elevated to an incident.

3. In case of events that will remain occurrence, the airline provides feedback to ESPs as a part of the positive security culture together with potential additional comments. It is essential to build and maintain communication and a strong security culture which will encourage further reporting. The level of reporting of security occurrences by ESPs could also be the KPI for assessing their SeMS maturity.

4. In case of events elevated to incidents, step 4 is the starting point of the security risk assessment performed by the airline-ISM (2023) (SEC 1.12.1 and 1.12.2). The risk assessment process described in Section 5 of this manual could be adapted and used by individual entities for the purposes of security report analysis. The incident can be further elevated to serious incident as a consequence of this risk assessment.

5. Events classified as serious incidents shall be reported to IATA, specifically IOSA Program, as well as any other relevant international or regional organizations

6. All incidents (including serious) shall be reported to the Appropriate Authority by airlines or ESPs (if SeMS compliant). Given the criticality of incident and serious incidents, immediate actions compensating high level of vulnerability should be implemented to bring the increased risk down to the acceptable level. Based on this, the decision to implement additional security measures might be taken and communicated to the ESP.

7. Whether additional measures have been implemented in step 6, monitoring and review processes should be implemented to inform risk assessment. Timelines for rectification should be agreed and monitored. Data referring to measuring the resolution period could be used to assess the general effectiveness of the SeMS, especially in relation to security functions provided by the ESPs. This data could be later submitted to the Appropriate Authority as an annual report evidencing maturity of Quality Assurance processes as a part of airline and/or ESP SeMS.

8. The Appropriate Authority will perform their official risk assessment of all received reports. This may be combined with other information sources to produce a more holistic threat landscape report. This in consequence may lead to mandating implementation of mitigation measures by the airline and/or ESP, as indicated in the final step 9.

Reference documents

ICAO Incident Reporting Guidance and Taxonomy (2022)
SeMS Aviation Community (requires access via aviationsecurity@iata.org)
IATA SeMS Manual (2025)
IATA Incident Data eXchange (IDX) safety and security incident data management program