POSITION PAPER

Security Occurrence Analysis (SeOA) and Security Incident Reporting (SeIR)

Executive Summary

The European Commission Regulation (EU) 2026/247 adopted on 02 February 2026 translates existing ICAO Annex 17 Standards 3.5.1 d) and 5.1.6 and ICAO Incident Reporting Guidance and Taxonomy (2022) into the European Regulatory framework. Consequently, all airlines operating within Europe, in addition to all European airport operators and entities responsible for implementing requirements of their respective national civil aviation security programmes, will be directly impacted.

As the provisions contained in section 19 of the Commission Regulation (EU) 2026/247 become applicable as from 1st January 2028, operators and entities, including the External Service Providers (ESPs) subcontracted by operators, and third parties to EU airlines and associated supply chains, should prepare themselves and develop harmonized and global implementation measures.

Airlines that have established a Safety Occurrence Reporting system in accordance with Regulation (EU) 376/2014, and that are aligned with safety and security provisions contained in the IOSA Standards Manual (ISM), should ensure that any new security requirements are aligned with existing safety related processes in order to avoid duplication or inconsistencies in reporting processes.

This position paper proposes key elements for a harmonized implementation of these provisions:

Development of an internal reporting system for collecting information on occurrences reported by personnel (provision 19.4), but also passengers or general public (definition of occurrence), including data quality checking to improve data consistency (provision 19.5).

- ⇨ Need to develop interface aligned with the common ICAO and EU classification of incidents
- ⇨ Need to create a subcategory for the occurrences reported by the personnel (operational deviation)
- ⇨ Need to develop an interface permitting data quality analysis

Security Occurrence Analysis (SeOA) determining which occurrence could be classified as incident, thus requiring further actions (provision 19.3).

- ⇨ Need to support occurrence analysis, potentially using AI tools, triggers and prioritization
- ⇨ Need to ensure timely analysis of all occurrences

Risk Assessment and determination of the severity (provision 19.3) of security incidents

- ⇨ Application of the principles of Operational Risk Management in Aviation Security
- ⇨ Application of common triggers for determining the severity of the security incident (see Table 1 below)
- ⇨ Need to create method to classify "serious security incident" based on harmonized triggers
- ⇨ All confirmed security incidents require immediate actions
- ⇨ All confirmed security incidents need to be treated and closed within 30 days

Mandatory Security Incident Reporting (SeIR) to the relevant authorities following reporting deadlines (provision 19.3) as well as a template and a common classification of incidents (provision 19.6).

- ⇨ All serious security incidents must be reported as soon as possible, and within 72 hours maximum
- ⇨ Operators could also report other (non-serious) security incidents if required to effectively resolve them
- ⇨ In addition, even the resolved (or closed) incidents must be reported to the authorities

Descriptors that could be considered as potential Triggers for Serious Security Incidents

- ⇨ Descriptors listed as "Category" in the ICAO Incident Reporting Guidance and Taxonomy (2022) and the Appendix V in the Commission Regulation (EU) 2026/247
- ⇨ Descriptors that could be directly linked to the different Articles 1 in the ICAO Aviation Security Instruments[1]. Conventions' Articles 1 legally define which unlawful and intentional offences could qualify as "act of unlawful interference" for ICAO official reporting.
- ⇨ *Note that at the date of the drafting, the Tokyo (1963) and The Hague (1970) conventions were ratified by 187 ICAO Contracting States, and the Montreal (1971) Convention together with its Supplementary Protocol (1988) by 190 and 178 States respectively (ICAO Composite Table – States of Treaties)*
- ⇨ All descriptors listed below are already included in the IATA Incident Data eXchange (IDX)

Table 1 – Proposed Triggers for Serious Security Incidents

#	Proposed Triggers for Serious Security Incident
1	**Hijacking in flight**
2	**Sabotage**
3	**Unruly passenger (to be considered for level 3 and 4 only to be reported)[2]**
4	**Discovery or use of prohibited items, improvised explosive device (IED), improvised incendiary device (IID), and/or undeclared Power Banks (if serious consequences and appropriate)**
5	**Chemical, biological and radiological (CBR) attack**
6	**Unplanned disruptions, including bomb threat or hoax (*on the ground*)**
7	**Bomb threat in flight (to be considered for amber and red levels)**
8	**Attack (non-UAV) against an aircraft (*in service or not*)**
9	**Attack against aircraft systems**
10	**Attack (non-UAV) on airport facilities**
11	**Attack against air traffic management (ATM) systems**
12	**Attack (non-UAV) against air traffic control (ATC) facilities**
13	**Attack against other critical systems and data**
14	**Damage to critical infrastructure/vulnerable points**
15	**Destruction or damage of air navigation aids**
16	**Unmanned aerial vehicle (UAV) caused threat against aircraft (*in service or not*)**
17	**UAV Near miss/Encounter with aircraft in flight**
18	**UAV Strike/Collision with aircraft in flight**
19	**UAV caused threat against airport infrastructure**
20	**UAV caused threat against passengers**

More details are provided in the following portions of this position paper.

For more information, please contact aviationsecurity@iata.org
Please register in the SeMS Aviation Community
Please visit the public IATA Aviation Security Page, and the IATA Position Papers
Please download the **Security Awareness and Reporting videos** (in 13 languages) posted on the folder (2020) See it Report it videos in the SeMS Aviation Community

[1] *ICAO International Security Conventions: Tokyo Convention, 1963; The Hague Convention, 1970 supplemented by Beijing Protocol, 2010; Montreal Convention, 1971 supplemented by Montreal Protocol, 1988; and Beijing Convention, 2010.*

[2] **Need to include the "attempt to open aircraft doors during flight" as Level 4 in Chapter 16 of the ICAO Aviation Security Manual (Doc 8973)**

Background

1. In March 2022, the ICAO AVSEC Panel endorsed new guidance material on the Reporting of Aviation Security Occurrences and Incidents that was developed in coordination with the ICAO Secretariat and relevant working groups of experts.

2. From June 2022, the new ICAO Incident Reporting Guidance and Taxonomy remains publicly available in the six ICAO languages and is intended to assist States and industry stakeholders in the implementation of harmonized reporting processes for aviation security occurrences and incidents, based on a common taxonomy.

3. IATA actively participated in the development of the ICAO guidance and fully supports ICAO guidance and its clear and harmonized taxonomy for reporting security occurrences and security incidents aimed at facilitating analysis, information sharing and overall proactive efforts for improving the system. The taxonomy is fully aligned with IATA taxonomies.

4. In December 2024, IATA published an initial Position Paper on Security Incident Reporting on the public Security website outlining the legal background for security incident reporting in both ICAO Annex 17 for States and the IATA Operational Safety Audit (IOSA) Standards Manual (ISM) for airlines, including the new guidance on the ICAO website and IATA SeMS Manual.

5. In April 2025, IATA published another position paper describing some challenges when Reporting of Aviation Security Occurrences and Incidents (2025), in particular the need for proper Analysis of Security Occurrences, the coordination between External Service Providers (ESPs) and Operators, and the difficulties in assessing the severity of security incidents.

6. In February 2026, the European Commission adopted a new Commission Regulation (EU) 2026/247 on 02 February 2026 that mandates, *inter alia*, Security Occurrences Analysis, as well as Security Incident Reporting for all operators and entities. This amendment to existing European Regulation (EC) 300/2008 was required considering ICAO Annex 17 Standards mandating a confidential reporting system for analysing security information provided by sources such as passengers, crew and ground personnel (Standard 3.5.1 (d)), as well as the definition of processes for the reporting of information concerning incidents (Standard 5.1.6). The new provisions are fully aligned with the ICAO Incident Reporting Guidance and Taxonomy (2022).

7. As the provisions mandating the reporting, in Section 19, are applicable as from 1st January 2028, the operators and entities must be prepared as soon as possible. It should be noted that all the new European provisions focusing on reporting are already included in the different IATA Operational Safety Audit (IOSA) Standards Manual (ISM) sections on Operational Reporting (ISM SEC 1.12), Management Review (ISM SEC 1.9), and Quality Management, Quality Assurance and Quality Control (ISM SEC 1.10), as part of the overall Security Management System (SeMS).

Security Occurrence Analysis (SeOA)

8. Provision 19.4 of Commission Regulation (EU) 2026/247 requires the establishment of "*an internal reporting system for the reporting of information on aviation security occurrences in a practical and timely manner*". According to Annex 17 Standard 3.5.1. d), that internal reporting system is designed for analysing security information provided by sources such as passengers, crew and ground personnel (Standard 3.5.1 (d)).

9. The 2022 ICAO definition for **security occurrence**, maintained in the EU Regulation, addresses *events and activities that appear to be abnormal, unusual, strange, etc. and that should be reported internally or directly to authorities through appropriate channels by any person*. The ICAO guidance provides 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*.

10. Provision 19.4 of Commission Regulation (EU) 2026/247 also mandates '*all personnel of operators and entities responsible for the implementation of the national civil aviation security programme shall report information on aviation security occurrences through such internal reporting system*". It should be noted that occurrences reported by the personnel of operators and entities are likely to be of a better quality than all other occurrences reported by the passengers or even the general public.

11. It is therefore proposed to differentiate the occurrences reported by any person of the public, from the ones reported by personnel that could be either a real **security occurrence**, or an **operational deviation** with less security concern:

    a. **Security Occurrence**: Any security-related event that may result in a reduced security outcome, may increase the operational risks or endangers the safety of passengers, crew, ground personnel and the general public, or is a potential compliance breach. This includes the identification or observation of a vulnerability in the protection of civil aviation against acts of unlawful interference.

    b. **Operational Deviation**: A reported observation that an applied security measure, process, or Standard Operating Procedure (SOP) is performing differently from its designed or required outcome. Usually identified by personnel performing operational security functions during routing activity, operational deviation could be reported by any personnel. Recorded as a precursor signal that may warrant immediate operational correction or procedural adjustment, including where the observation does not meet the threshold for elevation to security incident status.

        ⇨ **Operational deviations** are typically the occurrences reported by a trained and knowledgeable personnel as "***Deficiency in ...***" using the descriptors listed as "Category" in the ICAO Incident Reporting Guidance and Taxonomy (2022) and the Appendix V in the Commission Regulation (EU) 2026/247

12. All security occurrences should be analyzed by designated security officers, security managers, or security analysts of the receiving entities to determine whether additional actions may be required.

    a. Determination is usually achieved by taking a prima facie approach to establish whether the combination of human factors is involved and/or evidence of a more systemic vulnerability in the way measures and controls are applied to prevent occurrences.

    b. If an Artificial Intelligence (AI) tool is deployed during the first level analysis, key words such as a harmonized list of potential triggers identifying serious incidents should be used.

    c. If the prime facie analysis is benign, meaning that no investigation into the occurrence is warranted based on organization thresholds, then the occurrence is appropriately categorized as per established taxonomy for statistical purposes.

d. The occurrences reported by personnel, including Operational Deviations, should always be treated with caution and a sense of priority, as corrective measures may be required, even if the deviation is not elevated to the level of an incident. Good security culture recommends that the staff having reported the occurrence, or an operational deviation, should be provided with some feedback.

e. If the prima facie analysis reveals unacceptable aspects, the occurrence should be elevated to the status of security incident, from which further investigation is required.

f. The analysis of security occurrences and operational deviations must be performed in an expedite manner because of the mandatory deadlines for reporting incidents that may qualify as serious incidents.

Risk Assessments of Security Incidents

13. As mentioned in Provision 19.3 of Commission Regulation (EU) 2026/247, security occurrences (or deviations) could formally be elevated to security incidents after the proper analysis (investigation, confirmation) by designated security officers, security managers, or security analysts.

14. When an occurrence (or an operational deviation) is elevated to the level of security incident, it means that a breach, or a vulnerability in the existing system has been identified and confirmed (incident). This is often termed "realized risk" meaning that something wrong happened that could have been exploited for endangering the protection of civil aviation operations, and the safety of passengers, crew, ground personnel or the general public.

15. Provision 19.3 of Commission Regulation (EU) 2026/247 outlines the "*determination that additional action is required*" when a security incident is confirmed. As "realized risk" is generated, immediate treatment and corrective actions must be taken by operators (and entities). In this context, all confirmed security incidents have an "*immediate impact on the level of aviation security*" for operators (and entities) regardless of their severity. Therefore, the "immediacy" criteria may not be relevant for reporting deadlines.

16. Operators and entities that have adopted a Security Management System (SeMS) should consider elements such as root cause analysis, security risk assessment, or exercise to determine necessary corrective actions to treat the new identified risks, or which are required for regulatory compliance purposes. This also includes proper monitoring that should be performed to ensure effectiveness in preventing future incidents or occurrences, or operational deviations.

Severity Assessments of Security Incidents

17. Provision 19.3 of Commission Regulation (EU) 2026/247, mandates the reporting of aviation security incidents to the relevant authorities and clarifies that some security incidents "*may also result, and classified as such by the appropriate authority, in act[s] of unlawful interference to be reported to ICAO in accordance with Annex 17*", but also the Commission in accordance with Provision 19.1 of Commission Regulation (EU) 2026/247.

18. Provision 19.6 of Commission Regulation (EU) 2026/247 requires the mandatory reporting of security incidents to be performed using a template set out in Appendix IV and shall refer to the common classification as laid down in Appendix V.

19. This means that the severity of the security incidents should be based on the different categories of incidents, in determining which categories could lead, in the end of the official review process, to the qualification of "act of unlawful interference". The proposed "Triggers for Serious Security Incidents" are developed in Table 1 (page 2 of this document).

20. As for occurrences and operational deviation, it is proposed to differentiate "normal" security incidents from "serious" security incidents as follows:

    a. **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.

    b. **Serious Security Incident**: A security incident designated by a security official or manager, for which risk mitigation and corrective actions are determined to be necessary, and which is using one of the descriptors defined as "triggers for Serious Security Incident".

Security Incident Reporting (SeIR)

21. Provision 19.3 of Commission Regulation (EU) 2026/247, outlines deadlines for the mandatory reporting of security incidents, starting from the time when the underlying occurrence is reported through the internal reporting system refer to in provision 19.4.

22. As previously mentioned, all confirmed security incidents require immediate action from the operators, including treatment and corrective measures, as part of the SeMS.
    ⇨ This means that the "immediacy" criteria is difficult to apply for operators.

23. All serious security incidents must be reported to the relevant authorities as soon as possible, and within the 72 hours mentioned in provision 19.3. Given operational realities, identification of single-window portal used for mandatory reporting, and shared by all relevant authorities, would be beneficial.

24. Operators could also report to the relevant authorities certain security incidents that are not qualified as "serious" but still require official support for reaching rapid resolution.

25. All serious and non-serious security incidents remaining open, thus unresolved, after 30 days should also be reported to the relevant authorities.

26. All closed non-serious security incidents should not be reported, unless the relevant authorities specifically require so.