Conceptual Framework

Threat Assessment and Risk Management (SeMS key element)
1- Threat Assessment
2- Risk Assessment (=> Risk level)
3- Risk Management

linked to KPIs (Incident Reporting, Oversight QA/QC, Threat Assessment & Risk Management)

Global Aviation Threat Picture - Mainly initiated by States - ICAO Aviation Security Global Risk Context Statement (Doc 10108 - Restricted)

Threat identification - The identification of the ***capability*** and ***intent*** of a perpetrator to attack civil aviation with the potential to harm life, systems, information, environment and/or property.

Capability. Their ability to commit the act someone wish to undertake.

Intent. The desire someone may have to mount an attack

Threat Assessment - ICAO Annex 17 Standard 3.1.3

Sharing of relevant information with Operators ... - ICAO Annex 17 Standard 3.1.5

Periodic vulnerability assessments *at airports ... - **ICAO Annex 17 RP 3.1.4***

*... for **conducting effective risk assessments** during their operations - **ICAO Annex 17 Standard 3.1.5***

Consequences. The nature and scale of the impact of the specific attack, in human, economic, political, and reputational terms under a reasonable worst-case scenario.

Likelihood. The **probability** of an attack being attempted against a target, considering both the ***intent*** and ***capability*** of the perpetrator(s) to carry out successfully a credible ***threat scenario***.

Threat scenario. An identification and description of a **credible attack** comprising a **potential target**, the modus operandi and methods of attack, and the adversary (based on the role an adversary plays in the aviation system – passenger, non-travelling person, and / or insider). This should be **sufficiently detailed to permit accurate assessment and analysis**.

Threat Assessment *performed by SeMS Operators (as **SeMS key element**) using Open Sources, alternative sources, official information, NOTAMs, Operational information such as Incidents reported, Disruptive pax, INAD, etc.*

Potential Target (on the ground, ESPs installations and in the air, including Conflict Zones)

Current mitigation measures. **Current security system** (Preventive Security Measures, Resources, CONOPS, etc.) included in different National and Local Programs and deployed to counter the identified current global, national and local threats known by the authorities and stakeholders

Risks. The outcome of an overall ***risk assessment*** of a successful attack, taking into account the ***likelihood*** and ***consequences*** of the ***threat level*** *and* ***threat scenarios***, and considering the remaining ***vulnerabilities*** after assuming ***current mitigating measures*** have been implemented.

Vulnerability. Weakness that could be exploited and consequently increases the exposure and harm in case of an attack.

Vulnerability assessments

New and Emerging Threats

Serious Incidents

linked to incident reporting — *linked to IDX*

Security incidents *reported either internally or by **External Service Providers (ESPs)***

Risk Assessment. The process of identifying, analyzing, and ***evaluating risks*** associated with potential threats to operations. It involves determining the ***likelihood*** of a ***threat*** occurring and the potential ***consequences*** if it does. The goal is to understand the ***level of risk*** posed by different threats and to prioritize them based on their ***severity*** and ***probability***. This process helps in ***making informed decisions*** about where to allocate resources and implement security measures.

Risk level. Outcome of the ***risk evaluation*** or "risk score" performed through the ***risk assessment*** process.

Risk tolerance. The level of risk that is deemed tolerable (operationally and financially) for the Entity / Operator. (risk tolerance is linked to **Corporate decisions**)

Risk handling strategies. Corporate decisions or **models** on how to mitigate potential risks or **to not operate**.

Risks too high to operate. AVOID

Acceptable risk level.

Additional mitigation measures. Measures that should be added to the ***current security system*** *when **risk tolerance** is below the actual **risk level** assessed. New **risk evaluation** required after additional measures are deployed.*

Temporary measures. Additional measures deployed by the Operator until additional mitigation measures are incorporated into the local security system.

Residual risk. The overall final risk that is deemed tolerable by the Entity / Operator and that cannot be reduced further without engaging disproportionnate resources compared to the benefit gained or where the potential solution is impractical to implement due to local circumstances.

Insurances. *Final residual risks are usually covered via insurances (premium).*

Risk Management. Systematic process part of ***SeMS key elements*** of identifying, assessing, and mitigating risks to ensure the safety and security of operations. It involves a continuous cycle of monitoring and reviewing risks, implementing security measures, and adjusting strategies as needed. This is linked to Corporate decisions with the goal of maintaining the risks to an acceptable level (including insurances level) while ensuring efficient and financially sound operations.

Quality Control and Quality Assurance SeMS key element

Monitoring and Review

Relevance / Accuracy of the information collected

Overall Confidence? *Calculation of a **confidence coefficient** of the overall **Risk Management** process. How confident / comfortable are we with the end results?*

Need for randomness?

Real risks and responsibilities?

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***. A security incident may also result in an act of unlawful interference that would require additional reporting ***by the State (not the Operator)*** to ICAO as per Annex 17 Standard 5.3.1 and Appendix 42 to the ICAO *Aviation Security Manual* (Doc 8973 — Restricted).

Serious 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, and in case of which there are no, or only limited, or insufficient preventive measures remaining to avoid the accident, or if the accident was avoided only due to coincidence, or pure luck. As for security incident, serious incident may be officially reported as an act of unlawful interference by the State (not the Operator) to ICAO (read security incident definition).

Security taxonomy. IATA IDX taxonomy and ICAO Incident Reporting public guidance (*https://www.icao.int/Security/SFP/Pages/Incident-Reporting-Guidance-and-Taxonomy.aspx*).

IATA Security Department ©2025, Version 1, March 2025