Operational Risk Management in Aviation Security

All aviation organizations operate in dynamic environments subject to change due to various internal and external factors. These changes introduce uncertainty, which is understood as a deviation from what is expected. From an enterprise risk management perspective, uncertainty can lead to both positive and negative circumstances that impact an organization's ability to achieve its commercial goals and objectives. This dual nature of risk-encompassing both opportunities and threats-is central to business risk management.

A dedicated chapter titled “Threat Assessment, Risk Assessment and Risk Management” in the new edition of the IATA Security Management System (SeMS) Manual highlights the specific aspects of risk management for operators and their External Service Providers (ESPs). The concept of risk management is similarly explained in the IATA Integrated Risk and Resilience Management (IRRM) Manual.

Introduction

In business risk management, risk is defined as the effect of uncertainty on corporate objectives, encompassing both positive and negative deviations.

In the context of aviation security, the concept of risk is narrower, primarily focusing on negative changes, and does not consider uncertainty related to positive outcomes. This distinction arises from the protective mission of aviation security, which aims to safeguard passengers, crew, ground staff, assets, reputation and the general public from malicious and intentional actions that can cause harm. The objective is to prevent adverse events such as terrorism, sabotage, major disruptions, and other threats to the safety and security of aviation operations. Therefore, aviation security risk focuses solely on negative impacts.

Understanding these differences is foundational for further analysis of the aviation security risk management framework. By examining the definitions and approaches, we can develop a comprehensive understanding of how risk is managed in aviation security and present a summary of terminology, methodologies, and practices employed to identify, assess, and treat security risks, ensuring the protection of aviation operations against intentional threats.

Aviation security risk management, which is a key component of SeMS can also be a part of the process described in the IRRM as an Integrated Risk Management (IRM). In this context, while SeMS is about integrating security into the business, IRM is about integrating security with the business and its overall risk management framework.

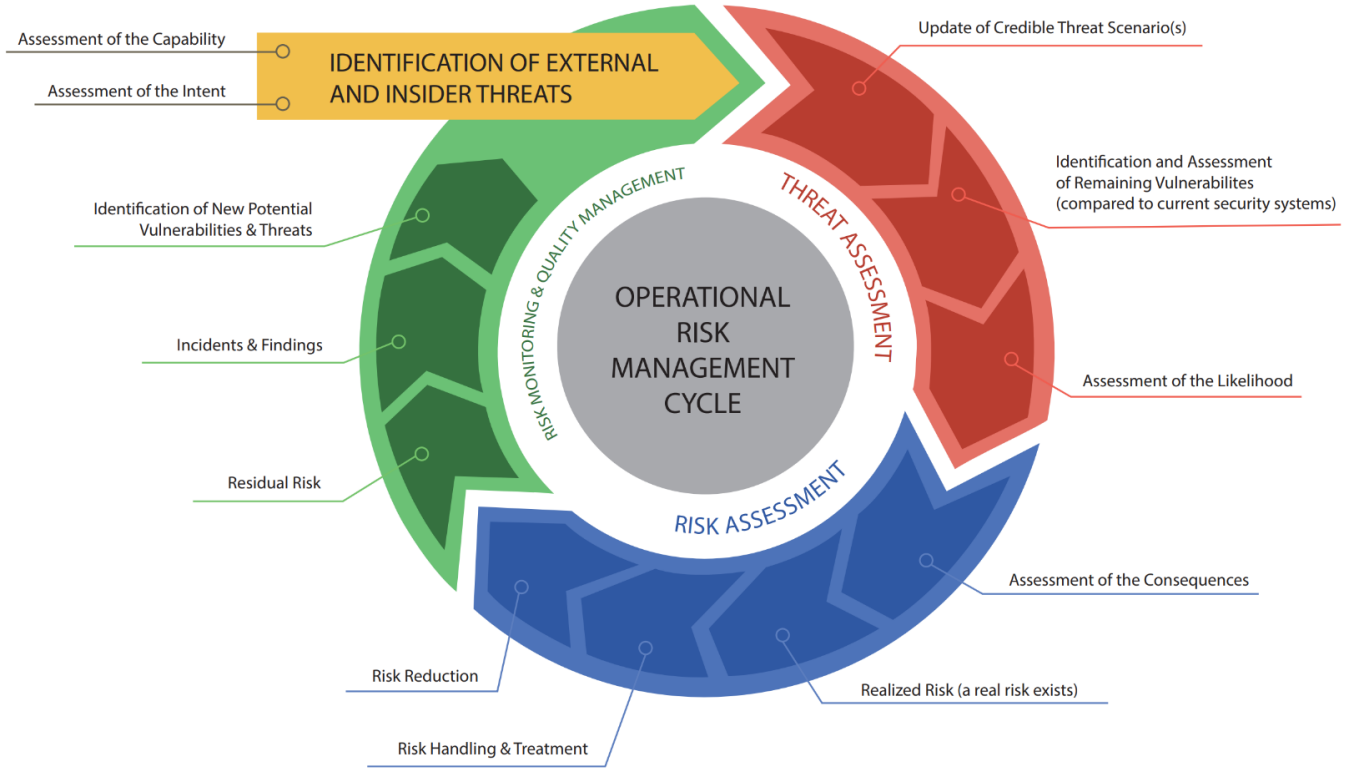
In other words, SeMS focuses on reducing security risks by identifying and managing them in collaboration with operational areas. IRM, on the other hand, involves security (and other areas) recognizing each other’s risks and opportunities to understand how they are interconnected.

SeMS helps manage and reduce security exposure by encouraging the business to recognize security elements within its operations (similar to safety). IRM adapts SeMS to influence more of the corporate thinking and blend with the corporate strategy. By integrating risk processes at the corporate level, security risk management ideally becomes more balanced between the typical “minimize losses” approach and a “take advantage of opportunities” business approach.

This document serves as an executive summary of the detailed explanations and guidance available in both the IATA SeMS and IRRM Manuals (IATA Security Manuals). For any questions, visit IATA Security and IATA Position Papers webpages, and register for the SeMS Aviation Community (by contacting aviationsecurity@iata.org).

Operational Risk Management Cycle

The following graphic summarizes the ongoing generic cycle of any Risk Management cycle which is defined as a systematic and structured process of identifying, treating and monitoring risks for ensuring the safety, security, regularity and efficiency of operations.



[Source: IATA SeMS Manual 2025]

Three key steps are identified in the above generic cycle, namely "Threat Assessment", "Risk Assessment" and "Risk Monitoring and Quality Management". Each of them is broken down into different key concepts linked to specific definitions.

A more detailed **conceptual framework**, along with all **relevant definitions**, for those seeking a deeper understanding of operational risk management challenges are available in the **Operational Risk Management folder** within the **SeMS Aviation Community** (register by contacting aviationsecurity@iata.org).

Threat Evaluation & Assessment

Threat assessment is typically conducted by analyzing a combination of information collected from open sources, alternative sources, official information (such as NOTAMs), or information shared by authorities with operators as mandated by ICAO Annex 17 (Standard 3.1.5). It may also include outcomes from operational functions, such as incident reporting from in-flight personnel (disruptive passengers, INAD, attempts of opening aircraft doors, etc.) or ground personnel, as well as the outcomes of quality management functions.

The objective of threat assessment is to evaluate potential threats and vulnerabilities for developing plausible threat scenarios.

Risk Assessment

When credible scenarios are developed, or updated based on proper threat assessments, the next step is to define the key parameters for assessing the risks. Risk assessment is a systematic and structured process of identifying, assessing, and evaluating risks, which then allow for the risk level to be specified in accordance with a method established by the organization. It is important to note that each organization may tailor its risk assessment method, including formulas or approaches, based on its own objectives and corporate culture.

In the context of aviation security, risks are usually defined as the exposure to an existing threat that could lead to a successful attack taking into account different parameters such as likelihood, consequences, and the vulnerability remaining after implementation of the measures contained in the current security system.

We need to identify the remaining vulnerabilities in the current security system protecting the potential target, and, in parallel, assess the likelihood of perpetrators willing to attack that target, as well as the potential consequences in case of a successful attack.

The likelihood, in the context of operational risk management, is defined as the probability of successful attack on a target, considering the intent (or motivations), combined with the capability (resources, weapons, etc.) of potential perpetrators when carrying out one of the credible threat scenarios defined earlier. Different formulas or approaches could apply for calculating likelihood.

Consequences are the measurement of all the impacts of a successful attack, usually considering the worse-case scenario. Again, the formulas for calculating consequences may differ depending on the importance of certain elements over others. The impacts could be human, economic, political or reputational in nature, thus inherently linked to each organization.

Identifying remaining vulnerabilities may also be challenging for organizations that do not have full visibility over the entire current security system deployed to protect the target.

If such risk assessment process does not identify a specific risk level, then the threat remains hypothetical, or the vulnerabilities and consequences not significant enough to necessitate immediate actions.

If such risk assessment identifies a level of risk, then the original security occurrence, vulnerability, or threat has materialized into a real security incident or risk with a specific risk level that needs to be first handled and treated by the organization, and then reported to the appropriate authorities.

The treatment of realized risk is linked to the risk tolerance, or the level of acceptable risk, as defined by each organization, followed by risk reduction processes. These processes may include the request for additional mitigation measures incorporated into the current security systems, and/or the deployment of temporary measures aimed at quickly reaching an acceptable level of risk.

The residual risk is defined as the final risk that is deemed acceptable by the organization appropriate to their operations to remain technically and financially viable. It could also be where the potential solution is impractical to implement due to local circumstances or constraints. These residual risks are usually covered by insurance premiums and require careful monitoring.

Risk Monitoring & Quality Management

When organizations decide to operate with residual risks, then risk management could be divided into two parts: risk monitoring, which ensures the safety, security, regularity and efficiency of all operations, and Quality Management, which comprises the usual SeMS Quality Control and Quality Assurance functions.

The objective is to continuously identify new potential threats and vulnerabilities, thereby initiating the first key step of the cycle again, which is a new Threat Evaluation and Assessment.