ICAO PAMPHLET: MANAGING INSIDER RISKS

ICAO's approach

The International Civil Aviation Organization (ICAO) understands the importance of ensuring those with knowledge of sensitive information and/or access to restricted areas of an airport do not exploit security measures, whether on purpose or by an unintentional act. ICAO continues to update and enhance Annex 17 – *Aviation Security* Standards and Recommended Practices (SARPs) and associated guidance material in the ICAO *Aviation Security Manual* (Doc 8973 — Restricted), including Standards on background checks, access control, use of explosives detection for screening of persons other than passengers, and staff screening.

Insiders in aviation... the risks they pose

An insider is any employee within an airport's operating environment, including those who are part of the supply chain. There are many different job roles with various levels of access and/or knowledge, including, but not limited to: security staff, airline employees, vendors, baggage handlers, cargo workers, taxi drivers, etc.

Of all the roles within an airport environment, it is important to identify those with levels of accessibility and/or knowledge that may pose a vulnerability. Of these roles, the vast majority of staff in those positions have no intention of exploiting those vulnerabilities to conduct or facilitate an attack or hostile act. However, an employee who may pose a **threat** can be categorized as one of these **types of insiders**:

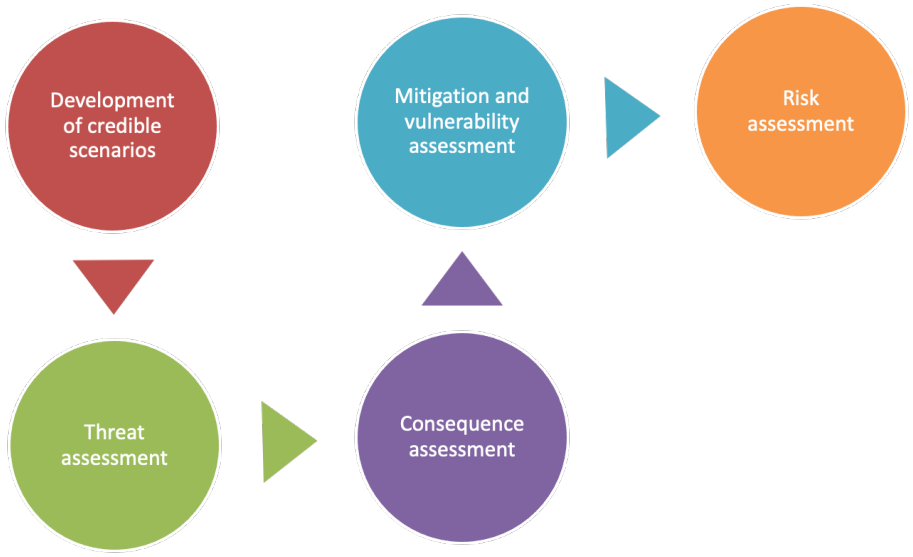
- those who are malicious and may be radicalized;
- those who are persuaded or coerced to act;
- those who are complacent by not doing their jobs well; and
- those who are ignorant of the motives of others or the consequences of their own actions.

The result of not properly mitigating the risks posed by insiders could lead to an act of unlawful interference causing serious harm to the aviation entity, which includes passengers, staff, aircraft, infrastructure, and the commercial operating environment of an airport.

ICAO Risk Assessment Model

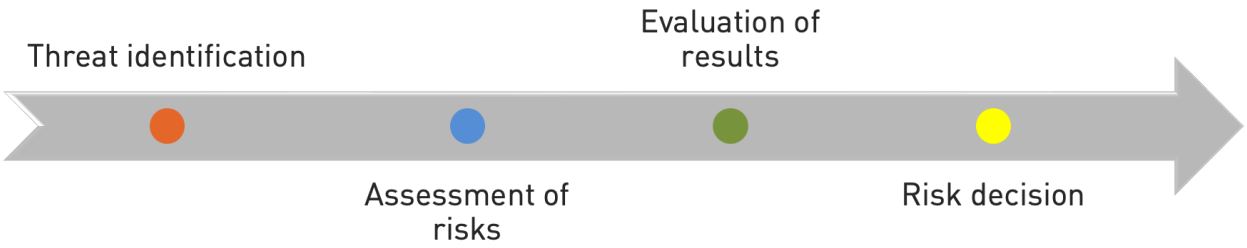
The Benefits of Risk Assessment

- Provides a systematic approach to examine and assess the key components of risk;
- Informs the effective allocation of limited resources;
- Provides the basis for prioritizing mitigation strategy alternatives;
- Assesses your security environment, focusing on keeping vulnerabilities at an acceptable level;
- Establishes a common framework for examining and communicating AVSEC issues, and determining priorities; and
- Provides the basis for compliance with Annex 17 – *Aviation Security* SARPs.



A threat scenario comprises the target (e.g. an aircraft), the method of attack (e.g. an improvised explosive device), and the adversary - the person attempting to conduct the attack. This could be a staff member – an **insider**. Their function depends on their role, what they do, what they carry, what they know, where they go, whether they are supervised and whether their work is checked.

It is important to differentiate between job roles to understand which ones are of concern and why and how to incorporate them into a wider risk assessment. Following the risk assessment, and taking into consideration the causes of identified vulnerabilities, action can be taken to mitigate the risks associated with insiders.



Mitigating action for insider-based risks

Informed by results of the risk assessment and an understanding of the causes of a vulnerability, a number of countermeasures are available to mitigate insider-based risks. These include:

Having a strong and effective security culture

Security culture is a set of security-related norms, values, attitudes, and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all personnel within an organization. From an aviation security perspective, this includes recognizing that effective security is essential to business success and ensuring security is a core value rather than an obligation or burdensome expense.

An effective security culture ensures that employees are engaged with, and take responsibility for, security issues. This should increase employee awareness of security issues; promote accountability and responsibility; reinforce the importance of undertaking security measures to the best of

their ability; and encourage reporting suspicious actions, items, or behaviours. In turn, this will provide fertile ground for the effective implementation of any new measures to address insider-based risks.

Personnel security policies, guidelines, and procedures before, during, and post-employment:

- background checks and vetting, which may include enhanced background checks involving analysis of intelligence-based information and monitoring of social media activities;
- training on security awareness for all employees within an airport, from leadership to staff in non-security functions, on a continuous basis;
- airport reporting programmes, to encourage the reporting of suspicious activities and communication of actions taken in response to these reports; and
- exit procedures when personnel end their employment, including an exit survey and procedures regarding the return of company property like airport identification cards, keys, mobile telephones, uniforms, and data (memory sticks, manuals, etc.).

Countermeasures in the landslide environment:

- surveillance and monitoring (e.g. vehicle licence-plate recognition, CCTV);
- patrols to identify suspicious behaviour and to act as a deterrent;
- targeted searches of vulnerable areas in the landside where large items can be disposed or hidden; and
- high visibility deterrent measures, such as the presence of dogs, police, military, and other persons that can be deployed at an airport.

Countermeasures within an airport for access control:

- security identification permit system (e.g. airport identification cards or passes), badge protocols, management, and access control procedures at all entrances to the airport, airside, and Security Restricted Areas (SRA), to include enhanced access controls such as biometrics and electronic access control systems;
- screening and searching to prevent prohibited articles from entering the SRA, applied to:
  - ✓ all employees;
  - ✓ their possessions, both personal possessions and tools of the trade;
  - ✓ vehicles and the items carried within when entering the SRA; and
  - ✓ equipment and items that employees have access to including aircraft, vehicles, hold baggage, catering, goods and cargo; and
- vehicle permits for entry into the airside and SRA.

Countermeasures in an aircraft:	• on the ground: searches, access control, protecting/guarding; and • on-board and in-flight: locked cockpit doors, air marshals.
Airspace security:	• emergency response procedures; and • military response.
Response:	• contingency planning and emergency response; • resilience planning; and • recovery and return to business as usual.

It is important to consider in an **insider risk mitigation strategy** how countermeasures can be implemented in a manner that is effective both in providing security value and in a unique operating environment.

Additional Information

For additional information on the ICAO Aviation Security Risk Assessment Process and Mitigating the Risks posed by Insiders, please refer to:

- **ICAO AVSEC Training:**
  - ✓ ICAO Risk Management Workshop
  - ✓ ICAO Insider Risk Workshop
- **ICAO Documents:**
  - ✓ ICAO *Aviation Security Manual* (Doc 8973 — Restricted)
  - ✓ ICAO *Aviation Security Global Risk Context Statement* (Doc 10108 — Restricted)

- **ICAO Tools and Resources:**

  ✓ ICAO Toolkit on Enhancing Security Culture

  ✓ ICAO Security Culture Campaign Starter Pack

  ✓ ICAO Insider Threat Toolkit


Edition 01 August 2022

ICAO

ICAO INSIDER THREAT TOOLKIT

GENERAL

This toolkit, created by the Aviation Security Panel's Working Group on Training, is designed to assist organizations operating in the aviation environment to better react to the ever-evolving insider threat. As noted in the ICAO *Aviation Security Global Risk Context Statement* (Doc 10108 - Restricted), terrorists consistently look to exploit vulnerabilities in security controls and commit acts of unlawful interference (AUI) against aviation, which could be facilitated through the exploitation of insiders.

Who are insiders?

Insiders are full or part-time employees (including contractors, temporary and self-employed personnel) who are working in or for the aviation sector whose role provides them with privileged access and/or knowledge to secured locations, items or sensitive security information.

What is the insider threat?

The insider threat refers to the risk arising from aviation employees conducting or facilitating an AUI through use of their authorized access, thereby giving them a tactical advantage.

What is the rationale of an insider?

Insiders may conduct or facilitate an AUI through a lack of awareness, complacency or maliciousness. Lack of awareness of policies and procedures and complacency (lax approach to policies and procedures) can cause insiders to unintentionally facilitate an AUI through their negligence, inaction or failure to follow security policies and procedures.

On the other hand, malicious insiders – those who make a conscious decision to conduct an AUI – may be driven by a mix of personal vulnerabilities, life events and situational factors, such as financial gain, ideology, revenge, desire for recognition, or coercion.

ICAO INSIDER THREAT TOOLKIT

- **ICAO Websites:**

  ✓ ICAO Security Culture website:https://www.icao.int/Security/Security-Culture/Pages/default.aspx


ICAO SECURITY AND FACILITATION

Search...

About ICAO | Global Priorities | Events | Information Resources | Careers | UnitingAviation | ICAO TV | Subscribe

ICAO / Security and Facilitation / Security Culture

Security Culture

Security Culture Platform

Articles

Best Practices and Guidance

Video Campaigns

Pamphlets and Other Campaigns

Security Culture

  ✓ ICAO Implementation Support and Development – Security (ISD-SEC) website: www.icao.int/Security/isd/Pages/default.aspx

For further information on this pamphlet and on the ICAO Insider Risk Workshop please contact:

ICAO AVSEC Assistance, Capacity Building and Training
Implementation Support and Development – Security (ISD-SEC)
ICAO HQ Montréal
Email: isd@icao.int