ICAO INSIDER THREAT TOOLKIT

GENERAL

This toolkit, developed by ICAO in collaboration with 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.

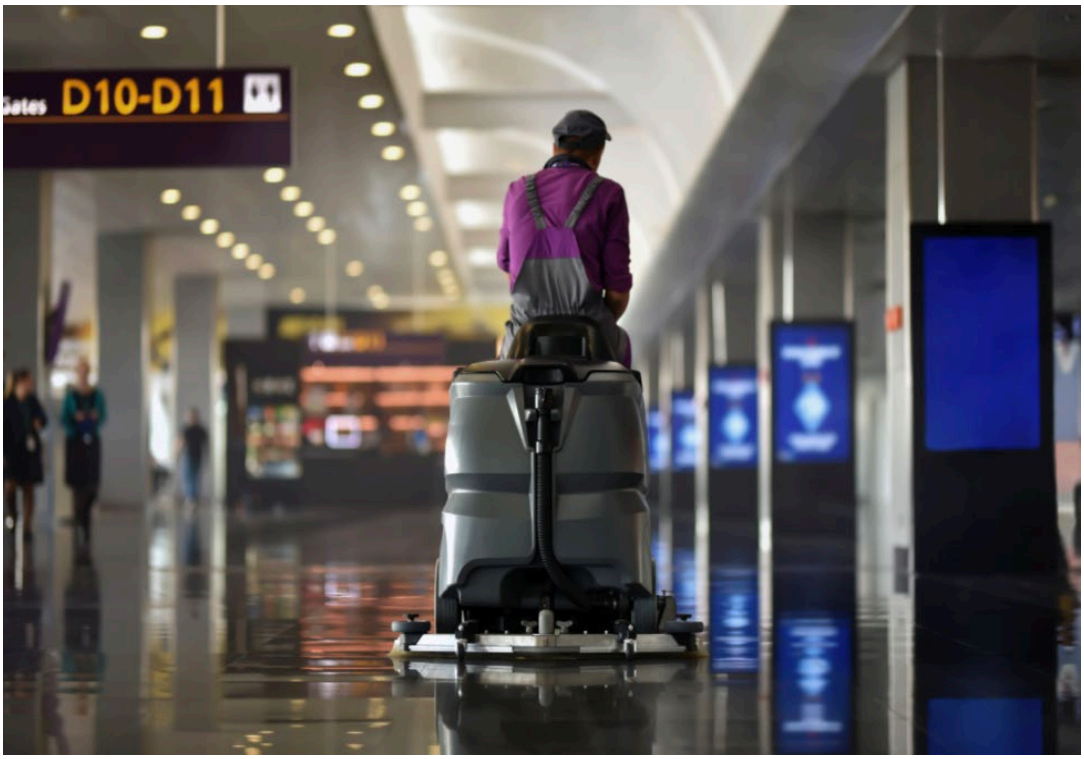
A malicious insider could deliberately seek to join an organization to conduct an AUI or acquire the intention of doing so during their employment (e.g. recruitment by a third party to exploit their trusted position).

How can Insiders act?

Insiders can conduct any AUI (e.g. destruction of an aircraft in service, introduction of a weapon or hazardous device or material intended for criminal purposes on board an aircraft or at an airport). Insiders can share confidential information, facilitate access to restricted areas, perform their roles inadequately enabling the introduction of prohibited articles into restricted areas, help external parties to obtain access to computer systems or other digital infrastructure[1], etc.

MITIGATION MEASURES

A range of personnel security measures and policies can help organizations mitigate the threat posed by insiders. In general, these measures seek to reduce the risk of recruiting staff who may present a security concern by their actions; minimize the likelihood of existing employees becoming a security concern; reduce the risk of insider activity; and protect an organization's assets.



[1] Digital Infrastructure means assets primarily related to mobile and internet communications.

Insider threat mitigation measures and tools can be grouped by the following areas.

BACKGROUND CHECKS AND VETTING

Policies and procedures: Robust policies and procedures on background checks, including employee's identity, previous work experience, criminal history and educational background, are a cornerstone of any framework aimed at mitigating the threat posed by insiders. Such policies and procedures must be clear and concise and should be periodically reviewed.

Initial background checks: All employees that need unescorted access to airside and security restricted areas, and persons with access to sensitive security information, must undergo background checks[2] as specified by the appropriate authority.

Initial background checks should cover:

- identity (e.g. provision of a passport, identity card, records of registry of birth, etc.);
- criminal history (to the full extent permissible by local regulations and laws);
- reference check (to attest to the work ethic and overall suitability of the prospective employee); and
- employment history (e.g. previous employers, educational history, etc.).

Recurrent background checks: Background checks should be recurrent and updated on a regular basis as part of cyclical personnel security checks. It is good practice to update a background check every time airport identification permits need to be renewed.

Those who commit an illegal act or AUI using insider access or knowledge often acquire the intention to do so after employment has been secured. Additionally, many insiders may have already attracted management's attention (e.g. through breaches of discipline and poor performance), which should be taken into consideration during the recurrent background check process.

Continuous vetting: A continuous vetting process should be encouraged, in collaboration with the relevant appropriate authorities (and where relevant, with authorities from other States). This is to assess whether an employee continues to meet applicable employment requirements.

[2] Standard 3.5.2 in Annex 17 - *Aviation Security* (Twelfth Edition, Amendment 18)

Enhanced background checks: Background checks that cover intelligence (and any other relevant information available on the suitability of a person to work in a function) could be useful. Indeed, States may collaborate with the relevant competent national authorities to incorporate some enhanced background check data into the layered background check and vetting process.

Equally, if staff identify suspicious or unusual behaviour in a person, then the relevant security and local competent authorities should be contacted, as an enhanced intelligence background check might be necessary.

TRAINING AND AWARENESS

Awareness training: Security awareness and security culture training should be encouraged for all staff. This will help ensure that all personnel know the security policies, standards, guidelines and procedures, as well as understand their purpose in maintaining a high level of security. This training will also enable new employees to develop the ability to identify and safely report suspicious behaviours to the appropriate authority or law enforcement officer/agency, including through anonymous means.

Training integration: Security awareness could be integrated into initial and existing recurrent training or through the use of campaign materials, workshops, drop-in sessions, etc., to promote a strong and effective security culture in aviation.

Role-specific training: For some staff, including but not limited to supervisors, managers and those with personnel security responsibilities, more in-depth, role-specific training will be appropriate to tailor targeted training outcomes.

Awareness campaigns: Visual messaging covering key security aspects should be developed for display within organizations and airport environments in order to serve as visual reminders to staff.

ACCESS CONTROL MEASURES

Screening: Access control measures should be in place to ensure that persons other than passengers, together with items carried, are screened prior to entry into airport security restricted areas[3]. Such screening should incorporate some random and unpredictable screening methods to offset insider knowledge and reduce the chance of prohibited articles being transported airside, including when carried by employees.

Policies and procedures: Policies and procedures should be clear and include:

- deactivate identification badges of employees who have left the organization (e.g. resigned, retired, etc.);
- limit access rights to restricted areas for pass holders based on strict operational needs;
- adequately protect the perimeter and access control points to ensure that staff security screening cannot be bypassed; and
- implement supervision protocols and wider use of closed-circuit television (CCTV) for operational activities, where appropriate.

[3] Standard 4.2.5 in Annex 17 - *Aviation Security* (Twelfth Edition, Amendment 18)

Review access lists: It is recommended that procedures for issuing airport identification permits are reviewed to ensure that the employee requesting access to a certain area has an operational need for such access.

PATROLLING

Random and unpredictable: Patrolling should be implemented in a random and unpredictable way, (e.g. spot checks), so that patrols cannot be avoided or bypassed as result of hostile reconnaissance or insider knowledge. Additionally, patrolling should not only focus on the surveillance of airport personnel but include passengers, other airport stakeholders, and airport infrastructure and goods for signs of unusual activity or poor security.

Patrolling can be effective as a visual deterrent if personnel are in uniform and use marked vehicles. Alternatively, patrolling can provide increased surveillance if conducted covertly.

SURVEILLANCE AND MONITORING

Methods: Quality control and monitoring of processes and employees specific to the insider threat can play an important role in avoiding or quickly addressing security incidents and AUIs. Methods of surveillance include CCTV, reviewing systems logs (e.g. access requests), and surveillance by staff on the ground.

Supervisors also play a critical role in recognizing and monitoring unusual activities and behaviours of the employees that they oversee.

Data: In some organizations, employee data can be found in various software application logs, which record the actions of employees. This digital data can highlight work patterns and be used as a tool to determine if any malicious intent exists amongst airport staff (e.g. accessing areas for which there is no operational need).

Applications could include:

- physical entry/exit logs, with a primary focus on time and access to physical spaces;
- log-on/log-off records, with a focus on time- and user-matching credentials;
- e-mail application logs; and
- database application logs.

REPORTING MECHANISMS

Reporting suspicious behaviour: Reporting mechanisms should involve everyone throughout the organization – not just those directly involved in security. These are important because employees are the 'eyes', 'ears' and 'voice' of an organization.

Reporting mechanisms may be set up so that employees can safely report suspicious behaviours or incidents through texts, emails, phone calls, internal communication channels, or by speaking to someone in person. Security reports should receive a clear, effective, and quick response.

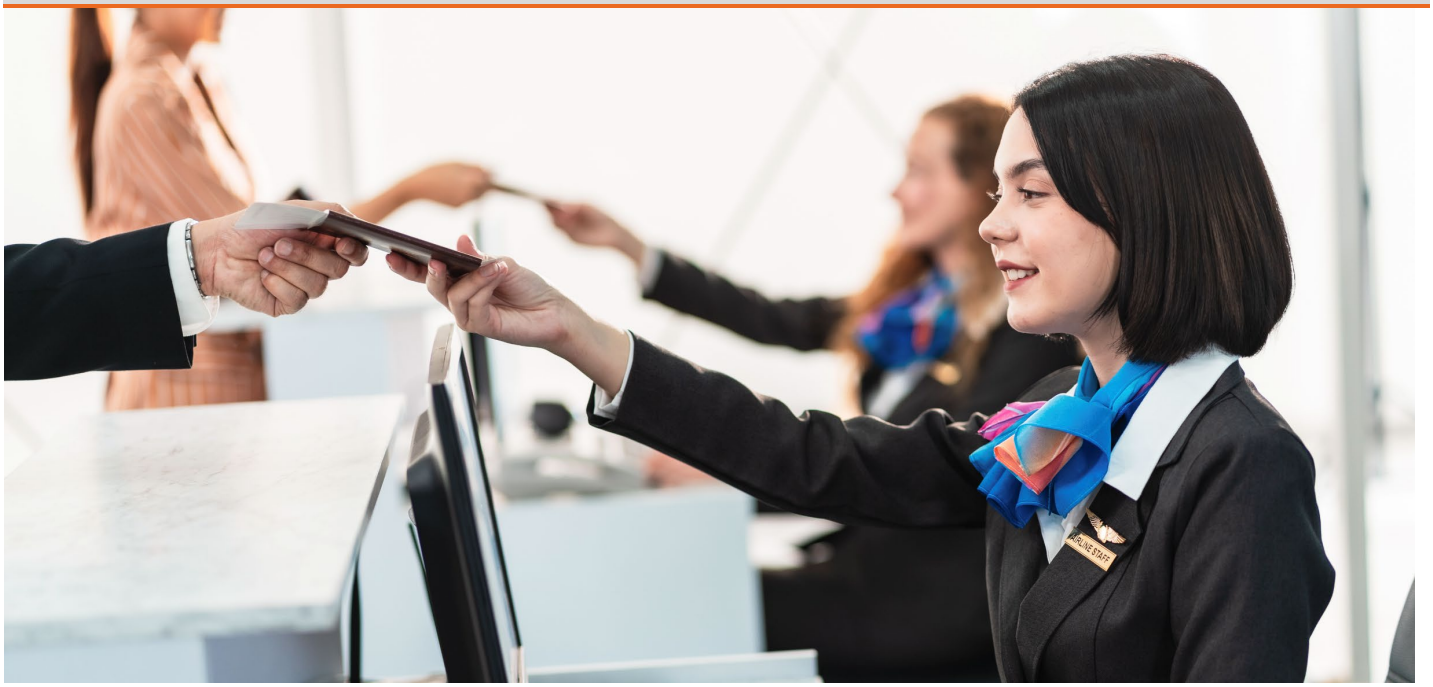
Anonymous or confidential reporting can be very useful to help mitigate potential insider threats and to establish an effective security culture in the organization.

BEHAVIOUR DETECTION[4]

Behaviour detection: A useful tool to help mitigate the insider threat can be behaviour detection. It is based on the premise that people may display signs of suspicious or unusual behaviour, and that these signs can be picked up by people who have been properly trained.

Training: Giving staff an understanding of what is suspicious activity and unusual behaviour, as well as an understanding of how to report it, can be a useful tool.

Behaviour detection training should be administered to a broad range of personnel, including, but not limited to, those involved in issuing passes, conducting background checks, and screening. However, all staff could benefit from this type of training as part of general security awareness training.



SECURITY CULTURE[5]

A strong and effective security culture: Establishing a positive security culture throughout the aviation sector is essential to mitigating insider threats and delivering effective and robust security outcomes. Employees can be:

- motivated and informed about insider risks through regular briefings on threats and wider security issues;
- trained to identify and report unusual or suspicious behaviours; and
- serve as a valuable source of information on vulnerabilities and how to address them.

[4] Behaviour detection is the application of techniques involving the recognition of behavioural characteristics, including but not limited to physiological or gestural signs indicative of anomalous behaviour (a combination of verbal and non-verbal signs) to identify persons with a potential intent to commit an act of unlawful interference.

[5] Additional information on security culture (including ICAO security culture resources) can be found on the ICAO Security Culture website at www.icao.int/Security/Security-Culture

LEADERSHIP AND STRATEGY

Strong leadership: It is critical that leaders understand their part in displaying positive security actions and behaviours expected from their workforce. Open communication between employees and management should be encouraged and leaders should have an understanding of the operational day-to-day pressures on the workforce, and the insider risks those pressures may create.

An executive (e.g. senior-level manager) who takes ownership of security risk principles, implements a top-down approach to security policies, and exemplifies expected behaviours is likely to promote a more compliant and consistent approach across the organization, further helping to mitigate insider threats.

Strategy: An insider threat mitigation strategy (endorsed by leadership) is recommended for helping employees understand how to recognize and how to report suspicious behaviours within the workplace.

The strategy can also include personnel-related insider policies, guidelines, and procedures. These include actions to be taken prior to employment and throughout an employee's time with the organization. The strategy and associated policies should be reviewed regularly with all key stakeholders.

Framework documents[6], handbooks and guidance material can be additional useful tools.

[6] e.g., www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework

HUMAN FACTORS

Human Performance and Factors: Organizations must have an understanding of how human performance can help mitigate the insider threat. This includes being aware of how human factors can impact individuals, who may either intentionally or unintentionally use their unique access to cause an AUI. Leaders and senior management should:

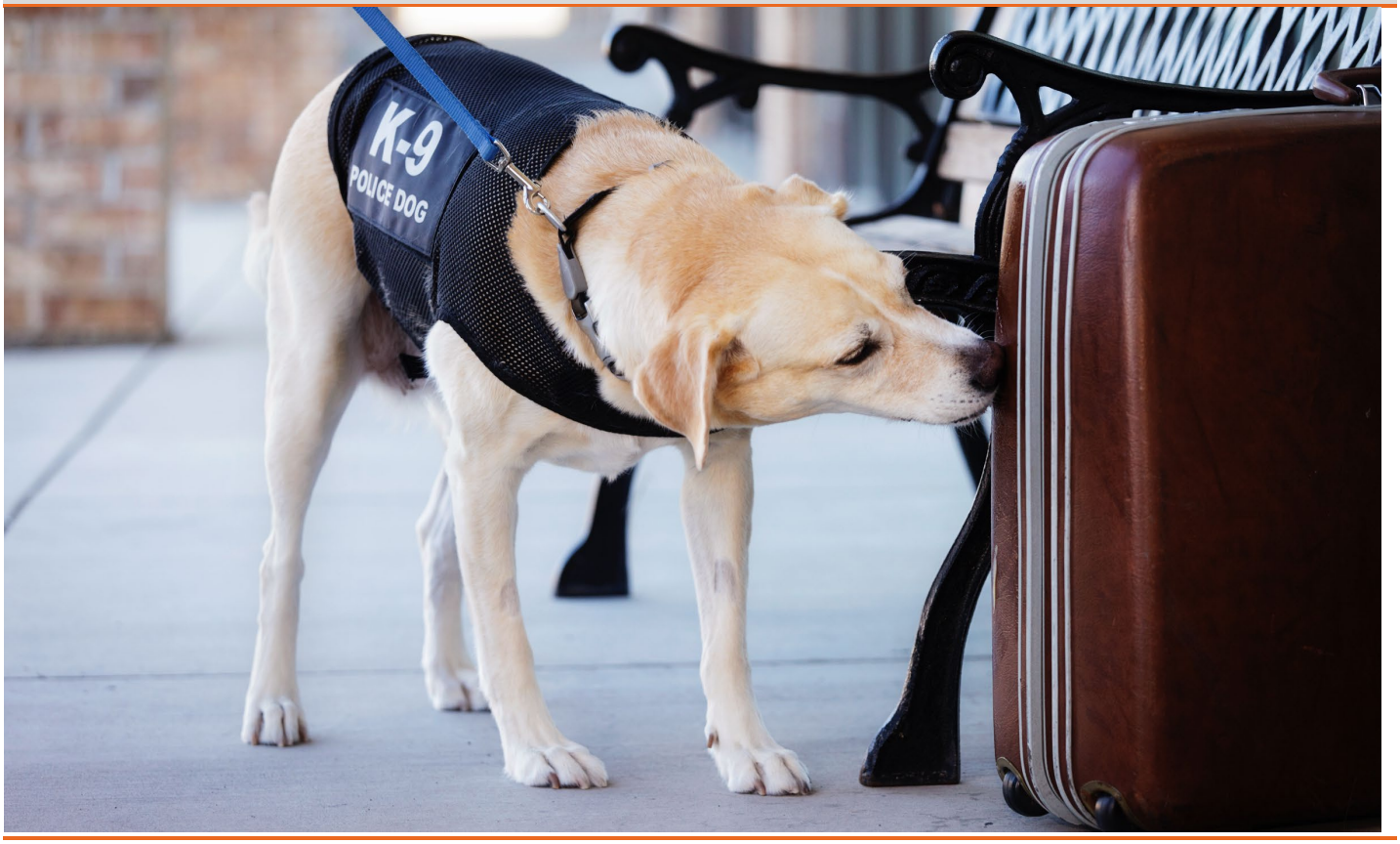
- develop an understanding of human capabilities and how these can help mitigate the risk of insider activity;
- understand human limitations and how these can be accommodated to ensure they do not impact performance;
- make it easy for staff to report security concerns and suspicious behaviours;
- understand the link between human factors, security culture and motivation;
- ensure the availability of resources needed by personnel;
- ensure supervisory staff are able to identify signs of stress and fatigue in order to deal with them promptly; and
- avoid complacency in day-to-day activities.

ADVANCED TECHNOLOGIES[7]

Explosive Trace Detection (ETD): Use of ETD machines can add an additional layer of security to the standard non-passenger screening procedures and/or random and unpredictable security countermeasures employed throughout the security restricted area, thereby helping to mitigate the insider threat.

[7] Application of advanced technologies may assist with mitigation of the insider risk through increased detection standards during the security screening process and/or by adding additional layers of security above the security baseline when applied in a random and unpredictable manner throughout the airport environment.

Explosive Detection Dogs (EDDs): EDD teams can be used to serve many purposes such as: security screening in all areas of the airport (landside, airside, passengers, non-passengers, baggage, cargo, etc.), sweeping security restricted areas and providing means of implementing random and unpredictable security measures.



Artificial Intelligence (AI): Use of AI-based systems by trained employees can help to identify trends and abnormal activities. E.g. modern incident management solutions can help identify incidents and differentiate mundane events from imminent threats, such as attempted break-ins into secured areas.

— END —