

---

Postgraduate Certificate in Aviation Security Management

## Aviation Security Risk Assessment

---

**\*\*Access control:\*\*** A security measure that restricts entry to authorized individuals only. This can be achieved through various means, such as keys, access cards, biometric identification, or security personnel.

**\*\*Adverse security threat:\*\*** A situation or event that could potentially harm aviation security, such as terrorist attacks, hijackings, or acts of sabotage.

**\*\*Aviation security (Avsec):\*\*** A set of measures and procedures designed to protect civil aviation against acts of unlawful interference, such as terrorist attacks, hijackings, or acts of sabotage.

**\*\*Aviation Security Management System (ASMS):\*\*** A systematic approach to managing aviation security risks, which includes the identification, assessment, and mitigation of those risks.

**\*\*Aviation Security Risk Assessment (ASRA):\*\*** A process of evaluating the likelihood and impact of potential security threats to civil aviation, and determining the appropriate level of security measures to mitigate those risks.

**\*\*Aviation Security Training Program (ASTP):\*\*** A training program developed by the International Civil Aviation Organization (ICAO) to provide standardized aviation security training to personnel involved in aviation security.

**\*\*Biometric identification:\*\*** A security measure that uses unique physical or behavioral characteristics, such as fingerprints, facial recognition, or iris scans, to identify individuals.

**\*\*Cabin baggage:\*\*** Baggage that is carried by a passenger onto the aircraft and stored in the cabin.

**\*\*Civil aviation:\*\*** The branch of aviation that deals with non-military and non-state aircraft, including commercial airlines, private planes, and helicopters.

**\*\*Contraband:\*\*** Items that are prohibited from being carried onto an aircraft, such as weapons, explosives, or dangerous goods.

**\*\*Critical infrastructure:\*\*** Systems, networks, and assets that are essential to the functioning of a society or economy, and therefore require special protection.

**\*\*Crowd management:\*\*** A security measure that involves controlling and monitoring the movement of people in and around an airport, to prevent overcrowding, stampedes, or other security threats.

**\*\*Cybersecurity:\*\*** A set of measures and procedures designed to protect electronic systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

**\*\*Deployment plan:\*\*** A plan that outlines the specific security measures and resources that will be used to

protect a particular aviation asset or event.

**\*\*Detection equipment:\*\*** Equipment used to detect the presence of weapons, explosives, or other contraband, such as x-ray machines, metal detectors, or trace detectors.

**\*\*Emergency response plan:\*\*** A plan that outlines the steps to be taken in the event of an emergency, such as a security breach, terrorist attack, or natural disaster.

**\*\*Explosive detection systems (EDS):\*\*** X-ray machines used to detect explosives in baggage.

**\*\*Explosive trace detection (ETD):\*\*** A device used to detect the presence of explosive residue on surfaces, such as hands or clothing.

**\*\*Foreign object debris (FOD):\*\*** Any object that is not supposed to be on an airport's operational areas, such as tools, parts, or debris, that can cause damage to aircraft or pose a safety hazard.

**\*\*Hijacking:\*\*** The unlawful seizure or taking control of an aircraft by force or threat of force.

**\*\*Human factors:\*\*** The study of how human behavior and decision-making can impact aviation security.

**\*\*Identity management:\*\*** A security measure that involves verifying the identity of individuals, such as passengers, employees, or contractors, to prevent unauthorized access to secure areas or systems.

**\*\*Incident reporting:\*\*** A process of reporting and recording security incidents, such as security breaches, thefts, or acts of sabotage, to improve aviation security and prevent future incidents.

**\*\*Insider threat:\*\*** A security threat that originates from within an organization, such as an employee or contractor who uses their access to commit a malicious act.

**\*\*Integrated security system:\*\*** A security system that combines multiple security measures, such as access control, surveillance, and detection, into a single, integrated system.

**\*\*International Civil Aviation Organization (ICAO):\*\*** A specialized agency of the United Nations that develops international standards and recommended practices for civil aviation.

**\*\*Landside:\*\*** The area of an airport that is accessible to the general public, such as the terminal building or parking lots.

**\*\*Law enforcement:\*\*** The agencies and personnel responsible for enforcing laws and maintaining order, such as police or security forces.

**\*\*Luggage:\*\*** Baggage that is checked in and stored in the cargo hold of an aircraft.

**\*\*National Civil Aviation Security Program (NCASP):\*\*** A national program that outlines the security measures and procedures for protecting civil aviation within a country.

**\*\*Operation:\*\*** A specific security measure or procedure, such as a patrol or a checkpoint.

**Physical security:** A security measure that involves protecting people, property, and assets from physical harm or damage, such as barriers, locks, or alarms.

**Profiling:** A security measure that involves selecting individuals for additional screening based on specific characteristics, such as behavior, appearance, or travel patterns.

**Risk:** The likelihood and impact of a security threat.

**Runway:** A designated area on an airport for the landing and takeoff of aircraft.

**Screening:** A security measure that involves inspecting individuals, baggage, or cargo for weapons, explosives, or other contraband.

**Security audit:** An evaluation of an organization's security measures and procedures, to identify areas for improvement and ensure compliance with regulations and standards.

**Security culture:** The shared values, attitudes, and practices related to security within an organization.

**Security plan:** A plan that outlines the security measures and procedures for protecting a specific aviation asset or event.

**Security procedures:** Specific steps and actions that are taken to ensure aviation security, such as passenger screening or cargo inspection.

**Security screening:** The process of inspecting individuals, baggage, or cargo for weapons, explosives, or other contraband.

**Security threat:** A situation or event that could potentially harm aviation security, such as terrorist attacks, hijackings, or acts of sabotage.

**Sensitive information:** Information that requires special protection due to its confidential or proprietary nature, such as passenger data or aircraft blueprints.

**Surveillance:** A security measure that involves monitoring and observing a specific area or asset to detect security threats.

**Threat assessment:** A process of evaluating the likelihood and impact of potential security threats, and determining the appropriate level of security measures to mitigate those risks.

**Training:** The process of educating and preparing personnel for their roles and responsibilities in aviation security.

**Unlawful interference:** Any act that jeopardizes the safety of civil aviation, such as terrorist attacks, hijackings, or acts of sabotage.

**Vulnerability assessment:** A process of identifying and evaluating weaknesses in an organization's security measures and procedures, to improve aviation security and prevent security threats.

**\*\*Weapons:\*\*** Objects that can be used to cause harm or damage, such as firearms, knives, or explosives.