Airspace Risk Assessment Management Checklist

The Airspace Risk Assessment Management Checklist is a comprehensive tool designed to assist aircraft operators in systematically identifying, evaluating, and mitigating risks associated with airspace operations.

This checklist is fundamental for ensuring the safety and security of flight operations, especially when flying over or near conflict zones, or in the event of sudden geopolitical changes or unexpected military activities during a routine flight.

The checklist provides a structured approach to airspace risk assessment, enabling aircraft operators to maintain a high level of situational awareness and preparedness. It covers various aspects of threat identification, information collection, validation, and threat assessment, ensuring that all realised risks are thoroughly evaluated and treated.

By following the checklist, aircraft operators can implement additional mitigated safety and security measures to protect passengers, crew, and aircraft, including protocols for avoiding high-risk areas, and communication strategies to stay informed about potential threats.

This checklist is also available in the IATA Airspace Risk Assessment Guidance (2024), in the IATA Position Papers & Press Release webpage, in the new edition of the IATA SeMS Manual (2025) and in the SeMS Aviation Community.

Please contact aviationsecurity@iata.org for joining the Community or for any question.

Self-Assessment | Management Checklist

Airspace Risk Assessment Management Checklist

1. Threat Identification

a. Establish Baseline Awareness	Evaluation	
Identify current services, past, and planned destinations within the aircraft operator's network.	Yes ☐	No ☐
Identify all flight planned diversion airfields based on aircraft performance parameters.	Yes ☐	No ☐
Identify all Flight Information Regions (FIRs) transited or operated point-to-point.	Yes ☐	No ☐
Review conflict zone-specific guidance from State of Registry CAA and foreign authorities.	Yes ☐	No ☐
Maintain awareness of current geopolitical situations, actors involved and assess potential hostilities.	Yes ☐	No ☐

2. Cognitive Models for Threat Identification

a. Consider the use of Cognitive models	Evaluation	
Cynefin Framework	Yes ☐	No ☐
OODA Loop	Yes ☐	No ☐
SWOT Analysis	Yes ☐	No ☐
Red Teaming	Yes ☐	No ☐
Scenario Planning	Yes ☐	No ☐
Black Sawn theory	Yes ☐	No ☐
VUCA Model	Yes ☐	No ☐

3. Information and Source Collection

a. Lagging Information	Evaluation	
Gather occurrence and incident reports, historical data, and post-event analyses.	Yes ☐	No ☐
Analyze patterns and trends in security incidents and benchmark against past data.	Yes ☐	No ☐

b. Leading Information	Evaluation	
Collect intelligence reports on emerging threat and risk forecasts.	Yes ☐	No ☐
Utilize early warning systems to detect potential threats.	Yes ☐	No ☐

4. Critical Information for Threat Identification

	Evaluation	
Current and historical airspace restriction (AIP, AIC, NOTAM, SFAR, CZIB).	Yes ☐	No ☐
Stability in the airspace and/or on the ground.	Yes ☐	No ☐
Profile of potential threat actors	Yes ☐	No ☐

Alert status of air defence forces.	Yes ☐	No ☐
Nature of ongoing militarized conflicts.	Yes ☐	No ☐
Use of militarized aircraft power.	Yes ☐	No ☐
Military equipment availability and access to anti-aircraft equipment.	Yes ☐	No ☐
Foreign policy statements of states towards another.	Yes ☐	No ☐

5. Validation of Information

a. Verify Information	**Evaluation**	
Confirm validity of information through state regulators or agencies.	Yes ☐	No ☐
Corroborate information across multiple sources.	Yes ☐	No ☐
Assess credibility and bias of sources.	Yes ☐	No ☐
Limit reliance on single-source information.	Yes ☐	No ☐

6. Intelligence Analysis and Modelling

a. Intelligence Cycle	**Evaluation**	
Collect, process, analyse, and disseminate security threat information.	Yes ☐	No ☐
Develop a comprehensive view of potential threats and enhance preparedness.	Yes ☐	No ☐

b. Predictive Models	**Evaluation**	
Utilize predictive models to forecast potential future events.	Yes ☐	No ☐
Examples include the Global Terrorism Database, ACLED, GFELT, world bank and IFM models, and social unrest models.	Yes ☐	No ☐

7. Threat Assessment

a. Evaluate Intent and Capability	**Evaluation**	
Assess threat actor’s intent to execute specific threat scenarios.	Yes ☐	No ☐
Evaluate threat actor’s access to material resources.	Yes ☐	No ☐
Consider weapons systems and their capabilities.	Yes ☐	No ☐

b. Unintentional Threats	**Evaluation**	
Assess the likelihood of unintentional threats due to misidentification or other factors.	Yes ☐	No ☐
Evaluate state and non-state actors’ ability to deconflict airspace	Yes ☐	No ☐

8. Threat Assessment Rating

a. Determine Threat Levels	**Evaluation**	
Use an Intent versus Capability matrix to identify threat levels (very Low to High).	Yes ☐	No ☐
Translate threat assessment outcomes into organizational threat levels (e.g., HIGH, MEDIUM, LOW).	Yes ☐	No ☐

b. Link to Risk Assessment	Evaluation	
Integrate with Safety Management Systems (SMS) and/or Security Management System (SeMS)	Yes ☐	No ☐
Conduct airspace risk assessments within existing risk management frameworks.	Yes ☐	No ☐
Identify specific hazards derived from identified threats.	Yes ☐	No ☐
Apply risk controls and monitor their effectiveness.	Yes ☐	No ☐

9. Key Performance Indicators (KPIs)

a. Establish Security KPIs	Evaluation	
Regularly review and communicate changes in risk assessment.	Yes ☐	No ☐
Ensure geopolitical competence within the organization.	Yes ☐	No ☐
Maintain appropriate governance structures.	Yes ☐	No ☐
Utilize external sources for independent information and advice.	Yes ☐	No ☐
Conduct annual crisis and contingency planning exercises.	Yes ☐	No ☐
Review and formally sign-off risk assessments periodically.	Yes ☐	No ☐

10. Review and Documentation

a. Regular Review	Evaluation	
Schedule regular reviews of airspace risk assessments.	Yes ☐	No ☐
Document key decisions made by the Head of Security and/or accountable manager	Yes ☐	No ☐

11. Governance and Communication

a. Establish Governance Body	Evaluation	
Form a security review committee with representatives from security, safety risk management, quality management, flight planning & dispatch, flight operations, legal, cybersecurity emergency management, and senior executives.	Yes ☐	No ☐
Ensure the committee has the authority to implement risk mitigation.	Yes ☐	No ☐

--- END ---