APPROVED

TSOLMON.J
DIRECTOR AND GENERAL INVESTIGATOR
AIRCRAFT ACCIDENT AND INCIDENT
INVESTIGATIONS BUREAU

PROCEDURE FOR RISK ASSESSMENT AND MANAGEMENT

Document reference	**AAIIB - 25 - 29**		
Date of approval:	year-	month-	day-
Reviewed by:	Name and Position	Date	Signature
Prepared by:	Name and Position	Date	Signature

Record of Amandments

Amendment No	Description of Amendment	Section affected	Name and position	Date	Signature

Distribution list

№	Document	Distrubuted to (Unit/Organization)
1		
2		
3		

PROCEDURE FOR RISK ASSESSMENT AND MANAGEMENT

1. Purpose

1.1 The purpose of this procedure is to establish a framework to identify, assess, and control risks, and to plan, implement, and monitor mitigation measures.

1.2 Risk management shall be applied across, but not limited to, occupational safety, information security, protection of evidence, operational continuity, and legal compliance.

2. Scope

2.1 This procedure shall apply to all organisational units, employees, contracted personnel, and, where applicable, cooperating entities of the organisation.

2.2 This procedure shall apply to the following activities:

- work at accident/incident sites, including the collection, preservation, and transportation of evidence;
- preparation of reports, publication of information, and exchange of information;
- use of equipment, calibration and maintenance, and use of personal protective equipment (PPE);
- management of information systems, data, and document version control;
- contracts, procurement, training, official travel, and international cooperation;
- amendments to internal rules, procedures, and instructions, and approval of new documents.

3. Definitions

3.1 Risk means the combination of the likelihood of an event or condition and the severity of its consequences that may adversely affect the achievement of objectives.

3.2 Hazard means a condition or object with the potential to cause injury, damage, loss of information, or non-compliance with legal requirements.

3.3 Risk level means the level of risk determined based on the assessment of likelihood and severity.

3.4 Risk register means a record of identified risks, including their assessment, mitigation measures, responsible persons, timelines, and implementation status.

4. Principles

4.1 Risk assessment shall be evidence-based, transparent, and conducted using a consistent and repeatable methodology.

4.2 Risk mitigation measures shall follow the hierarchy of controls (elimination → substitution → engineering controls → administrative controls → personal protective equipment (PPE)).

4.3 Residual risk following the implementation of mitigation measures shall remain within the organisation’s acceptable risk level (risk appetite).

5. Roles and responsibilities

5.1 The Director / Chief Investigator shall establish the risk management policy and risk appetite, and make decisions regarding high and unacceptable risks.

5.2 The Senior Investigator / Quality Assurance function shall ensure proper documentation of risk assessments, monitor the implementation of mitigation measures, and conduct internal audits and inspections.

5.3 Heads of units / process owners shall identify risks within their areas of responsibility, plan and implement mitigation measures, and report on their effectiveness.

5.4 The Risk Coordinator (if designated) shall maintain and consolidate the risk register, prepare reports, and provide training and methodological support.

5.5 All personnel shall report hazards and risks, complete risk assessments as required, and comply with established control measures.

6. Risk assessment requirements

6.1 A risk assessment shall be conducted in the following cases:

- introduction of new activities or processes;
- work at accident/incident sites, including missions and special operations;
- introduction of new equipment, software, or systems;
- significant changes to documents, procedures, or regulations;
- occurrence of serious safety incidents, accidents, or information breaches;
- engagement of external organisations, including contracting or outsourcing arrangements involving data or confidentiality.

7. Risk assessment methodology

7.1 Risks shall be assessed using a scoring scale of 1 to 5 for likelihood (P) and severity (I). The risk score (R) shall be calculated as:

$$R = P \times I$$

7.2 Likelihood (P) scale

Score	Description
1	Rare (may occur less than once per year)
2	Unlikely
3	Possible
4	Likely
5	Almost certain

7.3 Severity (I) scale

Score	Description
1	Negligible (no injury, minimal impact)
2	Minor (minor injury or limited impact)
3	Moderate (injury requiring medical attention or moderate operational impact)
4	Major (serious injury, significant operational disruption, or major loss)
5	Catastrophic (fatalities, severe damage, or complete operational failure)

7.4 Risk classification and control measures

Risk score R	Classification	Requirement
1–4	Low (green)	Routine control; record and monitor.
5–9	Medium (Yellow)	Plan and implement improvement measures.
10–16	High (Orange)	Management-approved mitigation measures; implementation shall be monitored.
17–25	Unacceptable (Red)	Suspend the activity and take immediate management action.

8. Process

8.1 Risk identification: Identify the process steps, personnel involved, operating environment, equipment, information, and applicable legal requirements, and compile a list of potential hazards.

8.2 Existing controls shall be documented, including procedures, checklists, training, personal protective equipment (PPE), calibration, access restrictions, confidentiality, authorization, and other relevant measures.

8.3 Initial risk assessment (Inherent risk): Assign likelihood (P) and severity (I) scores and calculate the risk score (R).

8.4 Mitigation planning: Define mitigation measures, including responsible persons, timelines, required resources, and performance criteria. For high and unacceptable risks, management approval shall be required.

8.5 Residual risk assessment: Following the implementation of mitigation measures, reassess likelihood (P) and severity (I) and ensure that the residual risk is reduced to an acceptable level.

8.6 Recording and approval: Complete Form RM-01, obtain signatures from relevant parties, and record the risk in the risk register (RM-02).

8.7 Monitoring and review: Monitor implementation and effectiveness within established timeframes and conduct a reassessment in the event of significant changes or non-compliance.

9. Risk reporting

9.1 The unit responsible for risk management shall prepare monthly and quarterly risk summary reports, including the status of high and unacceptable risks, overdue mitigation measures, lessons learned, and recommendations for improvement.

9.2 Any serious accident or incident, information breach, or condition affecting the protection of evidence shall be reported to management without delay.

10. Documentation and record retention

10.1 The following records shall be maintained and retained: RM-01 risk assessment forms, RM-02 risk register, and evidence of implementation of mitigation measures (e.g. records, reports, checklists, training records, photographs, and logs).

10.2 Retention period: [e.g. 5 years], or as specified in the organisation’s records retention policy.

10.3 Confidentiality: Access to investigation data, personal data, and sensitive system information shall be controlled and protected in accordance with established access levels.

11. Accountability

11.1 Any violation of this procedure, failure to report or concealment of risks, or failure to comply with established control measures shall be subject to disciplinary action in accordance with applicable laws and the organisation’s internal regulations.

12. FINAL PROVISIONS

12.1 This procedure shall enter into force on the date of its approval.

12.2 Monitoring of implementation and any required revisions shall be made in accordance with the Procedure for Amendments to Documents.

ATTACHMENTS

Attachment 1. Risk Assessment Form (RM-01)

Activity / Task						
Location						
Date						
Participant(s)						
Assessed by						
№	Hazard / Risk Description	Existing Controls	P	I	R=P×I	Proposed mitigation measures (Responsible Person/ timeline)

Post-Implementation Assessment (Residual Risk)

№	Evidence of Implemented Measures	P	I	R	Approval/ Decision
Assessed by (signature)		Reviewed by (signature)		Approved by (signature)	
Name: _____ Date: _____		Name: _____ Date: _____		Name: _____ Date: _____	

Attachment 2. Risk Register (RM-02)

№	Date	Risk/Hazard Description		P	I	R	Mitigation Measures / Status	Responsible person	Timeline/Remarks

Attachment 3. On-Site Risk Assessment Checklist (RM-03)

Instructions: Complete this checklist prior to work and update it on site as necessary. The results of this checklist shall be attached to RM-01.

Item	Yes / No	Remarks/Actions	Responsible person
PPE (helmet, safety glasses, gloves, face mask, etc.) available and of correct size			
Hazardous areas / traffic - protective controls in place			
Weather / environmental conditions - additional protection required			
Communication (radio/phone) - channels and contact list available			
Medical support / emergency response arrangements (emergency plan)			
Access authorization / credentials available			
Evidence protection (chain-of-custody forms, sealing, packaging)			
Photo / video / drone use - authorization and data handling procedures			
Information security - device encryption/passwords, portable storage controls			
Equipment - calibration valid and functioning properly			