ISMS Risk Treatment Plan

3.9 Risk Treatment Plan (RTP)

3.9.1 The ISM, in consultation with the Risk Owner, shall create an RTP for all risks requiring treatment, detailing:

- The selected treatment measures (controls) and their objectives.
- Defined, risk-based priorities and required resources.
- Agreed timelines and responsible Risk Owners.
- Compensation controls required during implementation delays (if any).

3.9.1.1 Scale Value Likelihood of Occurrence (LO)

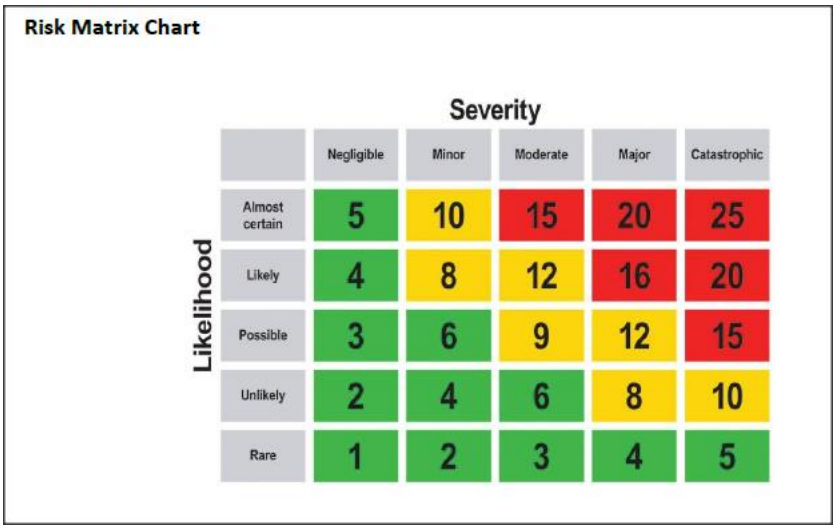
Value	Likelihood of Occurrence (LO)	ISMS Context Definition (Based on ISMM §3.5)
1	Rare	Highly unlikely to ever occur; no known vulnerability or credible threat vector.
2	Unlikely	Materialization is theoretically possible but not known to have occurred.
3	Possible	The threat scenario is possible; attack is credible and similar scenarios may have occurred before.
4	Likely	The threat scenario is likely/imminent; attack is feasible and similar scenarios have occurred often.
5	Almost Certain	Occurring frequently or is currently being actively exploited globally/within the sector.

3.9.1.2 Scale Value Severity of Outcome (SO)

Value	Severity of Outcome (SO)	ISMS Context Definition (Aligned with ISMM §3.5)
1	Negligible	Scenario causes negligible safety consequences and minimal business disruption or financial loss.

2	Minor	Minor operational disruption affecting security margins; temporary loss of non-critical data (Confidentiality/Integrity/Availability impact is recoverable with limited effort).
3	Moderate	Scenario that can cause or contribute to a safety Incident (e.g., minor operational disruption significantly affecting safety margins, maintenance procedural error, significant damage). Potential significant financial impact or regulatory fine.
4	Major	Major operational service outage; widespread compromise of safety-critical data Integrity or Availability. High likelihood of causing a safety Incident and significant business/reputational harm.
5	Catastrophic	Immediate or delayed scenario that can cause or contribute to an unsafe condition (e.g., fatal injury, major aircraft structural failure, total loss of control/critical system). Total loss of key maintenance records or critical systems leading to indefinite operational grounding.

RISK Assessment SCORE



If RAS is equal or greater than 12 (RAS > 12)

- Then the activity / operation can be undertaken only if appropriate safety management steps are taken to reduce the risk to acceptable levels.

If RAS is equal or less than 12 and greater than 6 (12 ≥ RAS > 6)

- Then reasonable safety management steps should be taken to further reduce the risk.

If RAS is less or equal to 6 (RAS ≤ 6)

- Then the risk is considered insignificant and safety management steps are not necessary / required.

3.9.2 Implementation and Effectiveness Check (IS.I.OR.210(a))

- Implementation: Risk Owners shall implement the technical, procedural, or organisational controls identified in the RTP in a timely manner.
- Effectiveness Check: The ISM shall periodically check the continued effectiveness of the implemented controls against the RTP objectives. This check should include validation against life cycle considerations (e.g., changes in technology or threat landscape).