Evaluating Operational Hazards, Threats & Vulnerabilities

This framework provides a structured approach to identifying, evaluating, and mitigating risks in intelligence operations. It follows a four-phase process: identify threats, assess vulnerability, evaluate impact, and develop mitigation options.

Phase 1 — Threat Identification

A threat is any actor, activity, or condition with the potential to cause harm. Threats must be identified before they can be assessed.

Threat Category	Examples	Key Questions to Ask
Human / Adversarial	Criminal networks, insider threats, espionage, terrorism	Who has capability and intent? What is their modus operandi?
Environmental / Natural	Natural disasters, infrastructure failure, pandemic	What hazards exist in the operating environment?
Technical / Cyber	Cyberattack, equipment failure, data breach, signal compromise	What systems are exposed? What dependencies exist?
Operational / Process	Human error, procedural failure, supply chain disruption	Where do process breakdowns most commonly occur?
Reputational / Political	Media exposure, political interference, legal action	What external actors could exploit or publicise vulnerabilities?

Phase 2 — Vulnerability Assessment

A vulnerability is a weakness that a threat could exploit. Rate each identified vulnerability using the scale below.

Rating	Score	Description	Indicator
Critical	5	Fundamental weakness — exploitation is straightforward with minimal resources.	No controls exist
High	4	Significant weakness — exploitation is feasible for a motivated adversary.	Controls exist but ineffective
Medium	3	Moderate weakness — exploitation requires some effort or specialised knowledge.	Controls partially effective

Rating	Score	Description	Indicator
Low	2	Minor weakness — exploitation requires significant skill or resources.	Controls mostly effective
Negligible	1	Minimal weakness — exploitation is highly unlikely under normal circumstances.	Strong controls in place

Phase 3 — Likelihood × Impact Risk Matrix

Plot each identified threat on the matrix by rating its likelihood of occurring and the impact if it does. Multiply the two scores to get the overall risk rating.

	Impact 1 Negligible	Impact 2 Minor	Impact 3 Moderate	Impact 4 Major	Impact 5 Catastrophic
Likelihood 5 Almost Certain	**5**	**10**	**15**	**20**	**25**
Likelihood 4 Likely	**4**	**8**	**12**	**16**	**20**
Likelihood 3 Possible	**3**	**6**	**9**	**12**	**15**
Likelihood 2 Unlikely	**2**	**4**	**6**	**8**	**10**
Likelihood 1 Rare	**1**	**2**	**3**	**4**	**5**

■ **Critical Risk (20–25)** ■ **High Risk (12–19)** ■ **Medium Risk (5–11)** ■ **Low Risk (1–4)**

Phase 4 — Risk Register

Complete a row for each identified risk. Prioritise treatment of Critical and High risks.

#	Threat / Risk	Likelihood (1–5)	Impact (1–5)	Risk Score	Treatment	Owner	Review Date
1	_____				■ Accept ■ Mitigate ■ Transfer ■ Avoid	_____	_____
2	_____				■ Accept ■ Mitigate ■ Transfer ■ Avoid	_____	_____
3	_____				■ Accept ■ Mitigate ■ Transfer ■ Avoid	_____	_____
4	_____				■ Accept ■ Mitigate ■ Transfer ■ Avoid	_____	_____

#	Threat / Risk	Likelihood (1–5)	Impact (1–5)	Risk Score	Treatment	Owner	Review Date
5	_____				■ Accept ■ Mitigate ■ Transfer ■ Avoid	_____	_____
6	_____				■ Accept ■ Mitigate ■ Transfer ■ Avoid	_____	_____
7	_____				■ Accept ■ Mitigate ■ Transfer ■ Avoid	_____	_____

Phase 5 — Mitigation Planning

Treatment Options

- ACCEPT — Document the risk and monitor. Suitable for low-rated risks where cost of treatment exceeds benefit.
- MITIGATE — Implement controls to reduce likelihood or impact. Most common treatment for medium and high risks.
- TRANSFER — Shift risk to another party (insurance, contractual obligations, outsourcing).
- AVOID — Cease the activity that creates the risk. Reserved for critical risks where no other treatment is viable.

Mitigation Controls Checklist

- ■ Physical security measures reviewed and updated.
- ■ Personnel screening and vetting procedures confirmed.
- ■ Information security controls (access, encryption, classification) assessed.
- ■ Operational security (OPSEC) plan reviewed against identified threats.
- ■ Contingency and continuity plans exist and have been tested.
- ■ Monitoring and early warning indicators established for critical risks.
- ■ Residual risk after controls has been formally accepted by appropriate authority.

Need a Different Format?

- An Excel version with automatic risk scoring formulas is available on request.
- Email: info@theintelanalystacademy.com.au — Subject: 'Risk Assessment Framework — Format Request'