Risk Management Policy

Document owner: Managing Director, Danpol Ltd.
Published: 1 December 2025
Scope: Corporate, project, financial, operational, HSEQ, cyber, and reputational risks.

1. Purpose

This policy sets the framework for identifying, assessing, controlling, and monitoring risks to Danpol's objectives. It aligns with ISO 31000, company governance requirements, and client frameworks.

2. Risk appetite

- **Safety & compliance:** Zero tolerance for uncontrolled life-safety or legal breaches.
- **Financial:** Moderate appetite for investments that improve capability, provided downside scenarios are mitigated.
- **Innovation:** High appetite for digital and process innovations when pilots include clear exit criteria.
- **Reputation:** Low appetite for behaviours that could undermine trust with clients or communities.

3. Roles and responsibilities

- **Board & Managing Director:** Approve appetite statements, review top risks quarterly, and ensure resourcing.
- **Risk & Assurance Lead:** Maintains the corporate risk register, facilitates workshops, and ensures integration with ISO systems.
- **Project managers:** Own project risk registers, track mitigations, and escalate issues exceeding tolerance.
- **All employees:** Report emerging risks, near misses, and improvement ideas via the governance portal.

4. Process

1. **Identify:** Workshops, lessons learned, PESTLE analysis, and trend data inform candidate risks.
2. **Assess:** Likelihood and impact scored using a 5x5 matrix covering cost, schedule, HSEQ, information security, and reputation.
3. **Treat:** Options include avoid, reduce, transfer, or accept. Controls documented with owners, budgets, and deadlines.

4. **Monitor:** Dashboards show residual risk ratings, overdue actions, and trigger events (leading indicators).
5. **Report:** Monthly project reviews, quarterly board packs, and CAS evidence submissions highlight status.

5. Integration

- Risk registers link to programme schedules, commercial forecasts, and digital assurance platforms.
- Change control ensures new scope or design variations are assessed before approval.
- Incident data from H&S, cyber, or quality systems automatically raises risk reviews.

6. Business continuity

Critical risks with potential for major disruption have contingency plans, scenario exercises, and recovery procedures aligned with the Business Continuity and Crisis Management Plan.

7. Review cadence

Policy reviewed annually or after significant events. Registers are audited twice yearly, with outputs stored in the Danpol policy vault.

Signed on behalf of Danpol Ltd.:

Daniel Nowakowski

Managing Director

1 December 2025

Digitally signed with authorisation stored in the Danpol policy vault.