Risk Management Capability Assessment Framework

Aligned to ISO 31000

Rating Logic

- N 🔴 – Absent: No to E1
- P 🟠 – Ad hoc: Yes to E1 only
- L 🔵 – Defined: Yes to E1 + E2
- F 🟢 – Operational: Yes to E1 + E2 + E3

---

1. Leadership & Commitment

Capability Criterion

Leadership actively sets direction for risk management and uses risk information to govern decisions.

Evidence Tests

- E1 – Direction:
- Is there documented leadership intent for risk management (policy, mandate, risk appetite, or expectations)?

- E2 – Enablement:
- Have leaders assigned accountability and provided resources to deliver that intent?

- E3 – Demonstration:
- Can leaders show recent decisions where risk information materially influenced outcomes?

---

2. Integration into Governance & Decision-Making

Capability Criterion

Risk management is embedded in governance, planning, and operational decision-making processes.

Evidence Tests

- E1 – Design:
- Are risk considerations explicitly built into governance, planning, and approval processes?

- E2 – Application:
- Are those processes consistently used with risk inputs in practice?

- E3 – Influence:
- Are decisions demonstrably changed, deferred, or reprioritised due to risk analysis?

---

3. Risk Management Framework Design

Capability Criterion

The organisation has a fit-for-purpose risk management framework tailored to its context.

Evidence Tests

- E1 – Existence:
- Is there a documented framework describing roles, processes, and interfaces?

- E2 – Fit:
- Is the framework tailored to organisational context, complexity, and risk profile?

- E3 – Usability:
- Do users apply the framework correctly without reliance on individual heroes?

---

4. Risk Identification

Capability Criterion

The organisation systematically identifies risks that could affect objectives.

Evidence Tests

- E1 – Method:
- Is there a defined method for identifying risks linked to objectives?

- E2 – Coverage:
- Are risks identified across strategic, operational, financial, and external domains?

- E3 – Currency:
- Are risks regularly refreshed to reflect change, not just historical issues?

---

5. Risk Analysis

Capability Criterion

Risks are analysed to understand causes, consequences, and uncertainty.

Evidence Tests

- E1 – Structure:
- Is there a defined approach for analysing likelihood, consequence, and drivers?

- E2 – Consistency:
- Is analysis applied consistently across the organisation?

- E3 – Insight:
- Does analysis reveal non-obvious vulnerabilities or exposure concentrations?

---

6. Risk Evaluation

Capability Criterion

The organisation evaluates risks to support prioritisation and decision-making.

Evidence Tests

- E1 – Criteria:
- Are risk criteria (including tolerance or appetite) defined?

- E2 – Application:
- Are risks evaluated against those criteria in practice?

- E3 – Decision Use:
- Are priorities and actions demonstrably aligned to evaluated risk levels?

---

7. Risk Treatment

Capability Criterion

Risk treatments are deliberately selected, implemented, and monitored.

Evidence Tests

- E1 – Options:
- Are treatment options identified and selected for material risks?

- E2 – Ownership:
- Are treatments assigned, resourced, and tracked?

- E3 – Effectiveness:
- Is there evidence that treatments reduce risk to intended levels?

---

8. Communication & Consultation

Capability Criterion

Risk information is communicated to the right people at the right time.

Evidence Tests

- E1 – Channels:
- Are there defined mechanisms for communicating risk information?

- E2 – Reach:
- Do relevant stakeholders receive and understand risk information?

- E3 – Engagement:
- Is there evidence of two-way dialogue influencing risk decisions?

---

9. Monitoring & Review

Capability Criterion

Risk management performance and risk exposure are actively monitored and reviewed.

Evidence Tests

- E1 – Measures:
- Are indicators defined to monitor risk and control performance?

- E2 – Review:
- Are risks and controls reviewed at planned intervals?

- E3 – Action:
- Do reviews lead to adjustments in risks, treatments, or controls?

---

10. Continual Improvement

Capability Criterion

The organisation learns from experience and improves its risk management capability.

Evidence Tests

- E1 – Feedback:
- Are incidents, near misses, and failures captured?

- E2 – Learning:
- Are lessons analysed and translated into improvements?

- E3 – Evolution:
- Can the organisation show measurable improvement in risk capability over time?