ISO 31000 Principles → Capability Criteria Mapping

1. Integrated

ISO intent: Risk management is part of governance, strategy, planning, and operations — not a side process.

Capability Criterion:

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

What “good” looks like (evidence):

- Risk explicitly considered in approvals, capital allocation, strategy refreshes
- Risk inputs required (and used) in decision forums
- Decisions demonstrably altered due to risk considerations

This is where hazard registers stop being enough.

---

2. Structured and Comprehensive

ISO intent: Risk is addressed systematically, not randomly or personality-driven.

Capability Criterion:

Risk processes are consistently designed, applied, and maintained across the organisation.

Evidence signals:

- Defined risk approach, roles, and escalation logic
- Consistent use of risk criteria and methods
- Comparable risk information across functions and levels

E1 = design, E2 = use logic fits perfectly here.

---

3. Customised

ISO intent: Risk management fits the organisation's context, objectives, and complexity.

Capability Criterion:

Risk management reflects organisational context, strategy, and risk appetite.

Evidence signals:

- Risk criteria aligned to strategic objectives
- Different treatment of strategic vs operational vs project risks
- Tailored depth — not "one register to rule them all"

This kills copy-paste risk frameworks stone dead.

---

4. Inclusive

ISO intent: Risk benefits from diverse perspectives and informed dialogue.

Capability Criterion:

Risk information is communicated to the right people at the right time, with two-way engagement.

Evidence signals:

- Defined communication channels
- Evidence of challenge, debate, and escalation
- Stakeholder input influencing risk decisions

Inclusion = engagement that changes thinking, not consultation theatre.

---

5. Dynamic

ISO intent: Risk management responds to change, uncertainty, and emerging risks.

Capability Criterion:

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

Evidence signals:

- Leading and lagging risk indicators
- Planned reviews triggered by change, not calendar only
- Adjustments to risks and treatments over time

Static risk registers fail this instantly.

---

6. Best Available Information

ISO intent: Decisions use timely, relevant, and transparent information — not perfect information.

Capability Criterion:

Risk decisions are informed by credible data, assumptions, and judgement.

Evidence signals:

- Clear assumptions and uncertainties documented
- Use of scenarios, ranges, or sensitivity
- Explicit acknowledgement of information limits

This is where decision quality > data quantity.

---

7. Human and Cultural Factors

ISO intent: Behaviour, incentives, and leadership matter as much as process.

Capability Criterion:

Leadership actively sets direction for risk management and models risk-aware behaviour.

Evidence signals:

- Clear leadership intent (policy, appetite, expectations)
- Accountability assigned and resourced
- Leaders can point to decisions shaped by risk

This separates “tone at the top” from “tone in the room”.

---

8. Continual Improvement

ISO intent: Risk capability improves through learning, not just compliance.

Capability Criterion:

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

Evidence signals:

- Incidents, near misses, and failures captured
- Lessons analysed and translated into changes
- Measurable improvement in risk capability over time

E3 = evolution is textbook ISO 31000.