ISO 31000:2018 Risk Management Checklist

A practical checklist for aligning your risk management process to the ISO 31000 framework

ISO 31000 · Risk Management · Risk Assessment · Risk Treatment · COSO ERM · King V

ISO 31000 is a guideline, not a certifiable standard — there is no audit to pass. This checklist sets out a practical sequence for aligning your risk management framework and process to ISO 31000's principles, so risk decisions are consistent, traceable, and embedded in how the organisation operates.

A Principles & Mandate

- [ ] Confirm risk management is integrated into governance and decision-making, not run as a separate exercise
- [ ] Secure a mandate and commitment from the board or top management
- [ ] Define how risk management creates and protects value for the organisation
- [ ] Communicate the purpose and scope of the risk management framework to stakeholders

B Framework Design

- [ ] Define the risk management policy, objectives, and accountabilities
- [ ] Integrate the risk framework into strategic and operational planning processes
- [ ] Allocate resources for risk management activities and tools
- [ ] Establish internal and external communication and reporting mechanisms

C Establishing the Context

- [ ] Define the external context, including regulatory, market, and stakeholder factors
- [ ] Define the internal context, including strategy, structure, and capability
- [ ] Set risk criteria, including how likelihood, impact, and risk appetite are defined
- [ ] Confirm the scope of each risk assessment before it begins

D Risk Assessment — Identification

- [ ] Identify risks systematically across strategic, operational, financial, and compliance categories
- [ ] Involve relevant risk owners and subject matter experts in identification
- [ ] Capture emerging and interconnected risks, not only known historical risks
- [ ] Record risk sources, causes, and potential consequences clearly

E Risk Assessment — Analysis & Evaluation

- [ ] Analyse likelihood and consequence using a consistent, defined scoring model
- [ ] Consider existing controls when analysing residual risk
- [ ] Evaluate risks against risk criteria to prioritise treatment
- [ ] Compare risk levels against defined risk appetite and tolerance thresholds

F Risk Treatment

- [ ] Select treatment options — avoid, mitigate, transfer, or accept — with clear rationale
- [ ] Assign treatment actions to named owners with realistic timeframes
- [ ] Assess residual risk after treatment actions are implemented
- [ ] Confirm treatment actions are resourced and do not introduce new risks

G Monitoring & Review

- [ ] Monitor key risk indicators on a defined frequency
- [ ] Review the effectiveness of controls and treatment actions regularly
- [ ] Reassess risks after significant internal or external changes
- [ ] Escalate risk appetite breaches through defined governance channels

H Recording, Reporting & Improvement

- [ ] Maintain a risk register that records assessment, treatment, and review history
- [ ] Report risk status to management and the board in a consistent format
- [ ] Capture lessons learned from realised risks and near misses
- [ ] Review and improve the risk framework based on performance and changing context