Risk Management Checklist

A practical, ISO-aligned checklist for identifying, assessing, treating and reporting risk on one register

ISO 31000 · COSO · ISO 9001 · ISO 14001 · ISO 45001 · ISO 27001

Risk management breaks down when registers live in spreadsheets, scoring is inconsistent between teams, and mitigation actions go untracked. This checklist sets out a practical, repeatable sequence for identifying, assessing, treating and reporting risk on a single, auditable register, aligned to ISO 31000 and COSO.

A Risk Identification

- [ ] Identify risks systematically across operational, financial, safety and compliance categories
- [ ] Involve risk owners and subject matter experts, not just a central risk team
- [ ] Capture the risk source, potential cause and consequence in clear, consistent language
- [ ] Record new and emerging risks as they arise, not only during periodic reviews

B Risk Assessment

- [ ] Assess likelihood and impact using one defined, consistent scoring model
- [ ] Score inherent risk before controls, then residual risk after existing controls
- [ ] Compare assessed risk levels against defined risk appetite and tolerance
- [ ] Re-score risks whenever circumstances or controls materially change

C Control Definition

- [ ] Define the specific controls that mitigate each identified risk
- [ ] Link every control to the risk(s) it addresses, not the other way round
- [ ] Assign a control owner accountable for its ongoing operation
- [ ] Distinguish preventive controls from detective and corrective controls

D Action Tracking

- [ ] Assign mitigation actions to a named owner with a realistic due date
- [ ] Track action status through to verified completion, not just "closed"
- [ ] Escalate overdue or at-risk actions through defined governance channels
- [ ] Confirm completed actions actually reduced the residual risk score

E Monitoring & Reporting

- [ ] Monitor risk exposure and key risk indicators on a defined frequency
- [ ] Report risk and control effectiveness to management in a consistent format
- [ ] Flag risk appetite breaches for escalation rather than waiting for the next cycle
- [ ] Review the risk register after audits, incidents or significant operational change

F Continuous Improvement

- [ ] Benchmark risk exposure trends period over period
- [ ] Feed audit findings and incident data back into the risk register
- [ ] Review and refine the scoring model as the risk landscape evolves
- [ ] Confirm the register remains a single source of truth across all business units