

Enterprise Risk Management (ERM) Readiness & Assessment Checklist

A structured checklist to assess ERM readiness — framework, identification, assessment, treatment, monitoring, reporting, and integration.

ISO 31000 • COSO ERM • King V

Use this checklist to run a structured enterprise risk management assessment end to end — from framework governance through risk identification, assessment, treatment, monitoring, reporting, and continuous improvement.

A Governance & Risk Framework

- ☐ Define risk management framework
- ☐ Establish risk governance structure
- ☐ Define risk roles and responsibilities
- ☐ Ensure board oversight of risk

B Risk Identification

- ☐ Identify strategic risks
- ☐ Identify operational risks
- ☐ Identify financial risks
- ☐ Identify compliance risks

C Risk Assessment

- ☐ Assess likelihood and impact
- ☐ Define risk scoring methodology
- ☐ Determine risk appetite and tolerance
- ☐ Prioritise risks

D Risk Treatment

- ☐ Define risk treatment plans
- ☐ Assign action owners
- ☐ Set timelines for actions
- ☐ Track risk mitigation actions

E Risk Monitoring

- ☐ Monitor risk indicators
- ☐ Track risk changes over time
- ☐ Escalate critical risks
- ☐ Review risk register regularly

F Reporting & Communication

- ☐ Provide risk dashboards
- ☐ Report to management and board
- ☐ Ensure transparency of risks
- ☐ Communicate risk information

G Integration

- ☐ Link risks to controls
- ☐ Link risks to audits
- ☐ Integrate risk with compliance
- ☐ Align risk with strategy

H Continuous Improvement

- ☐ Review risk framework
- ☐ Update risk methodology
- ☐ Improve risk processes
- ☐ Ensure ongoing monitoring