Risk Register Template & Field Checklist

The fields and structure a risk register needs before it can replace a spreadsheet

ISO 31000 · COSO ERM · King V · Risk Register

A risk register template is only as useful as the fields it forces you to fill in. This checklist sets out the structure a working risk register actually needs — the same structure XGRC® ERM runs live, with an audit trail on every change.

A Core Risk Fields

- ☐ Risk description written in plain language, not a category label alone
- ☐ Risk category (strategic, operational, financial, compliance)
- ☐ A named individual owner — never a department or a team
- ☐ Date first logged and date of last review

B Scoring Consistency

- ☐ One agreed likelihood scale, defined before the first risk is logged
- ☐ One agreed impact scale, applied the same way across every business unit
- ☐ A documented risk appetite and tolerance threshold for each risk category
- ☐ Inherent risk score recorded separately from residual risk score

C Controls & Treatment

- ☐ Existing controls listed against each risk, not assumed
- ☐ Residual risk score calculated after existing controls are accounted for
- ☐ A treatment decision recorded — avoid, mitigate, transfer or accept — with rationale
- ☐ Treatment actions assigned to a named owner with a realistic due date

D Linkage

- ☐ Each risk linked to the controls meant to manage it
- ☐ Each risk linked to any open treatment action addressing it
- ☐ Each risk linked to related audit findings, where one exists
- ☐ Risks connected to the strategic objective or process they threaten

E Review Cadence

- ☐ A defined review frequency per risk, not one blanket annual review
- ☐ A mechanism to reassess a risk after a significant internal or external change
- ☐ An escalation path when a risk breaches its appetite threshold
- ☐ A record of who reviewed the risk and what changed at each review

F Reporting & Governance

- ☐ A board-ready rollup available without manual compilation
- ☐ Risk trend visible over time, not just a point-in-time snapshot
- ☐ A single source of truth — no parallel or duplicate versions in circulation
- ☐ An audit trail of every change: who changed what, and when

G What a Spreadsheet Register Cannot Do

- ☐ Prevent two people editing the same risk at the same time
- ☐ Record who changed a rating and why, automatically
- ☐ Alert anyone the moment a risk breaches its appetite threshold
- ☐ Link a risk to its controls and actions in a way that stays in sync as they change