

OUTLIERS RISK MANAGEMENT CENTRE™

Risk Governance Toolkit™

Structure risk authority, accountability and oversight

Board / CRO / Internal Audit · Access Tier T2 · Flagship Edition 2026

Publication-ready resource for the Outliers Resource Library

1. Full Guide

Risk governance defines how authority, accountability and oversight for risk are structured and exercised. Strong governance ensures the right risks reach the right people with the right information at the right time. This toolkit provides the three-lines model, committee mandates, delegation, escalation and assurance mapping.

Three lines of defence

Line	Who	Responsibility
First line	Business & process owners	Own and manage risk in day-to-day operations
Second line	Risk & compliance functions	Set framework, oversee, challenge, aggregate
Third line	Internal audit	Independent assurance over the whole system

Maturity model

L1 Fragile	L2 Functional	L3 Disciplined	L4 Strategic	L5 Resilient
Informal / reactive	Basic, siloed	Standardised & governed	Integrated & quantified	Predictive & embedded

2. Templates

2.1 Risk governance RACI

Activity	Responsible	Accountable	Consulted	Informed
Set risk appetite	CRO	Board	Exec	All staff
Maintain risk register	Risk owners	CRO	2nd line	Risk Committee
Approve risk policy	CRO	Board	Risk Committee	Management
Test key controls	Control owners	CRO	Internal Audit	Risk Committee
Independent assurance	Internal Audit	Audit Committee	CRO	Board
Escalate breaches	Risk owners	CRO	Risk Committee	Board

2.2 Risk policy hierarchy

- Board Risk Charter (overarching mandate)
- Risk Management Policy (framework & appetite)
- Domain policies (credit, cyber, fraud, BCM, etc.)
- Procedures & standards (operational detail)
- Registers, KRIs and reporting (execution)

2.3 Delegated authority & escalation matrix

Decision / event	Authority	Escalate to	Trigger
Risk within appetite	Risk owner	—	Routine
Approaching limit (≥90%)	Function head	CRO	KRI amber
Limit breach	CRO	Risk Committee	KRI red
Material/critical risk crystallises	CRO	Board / Crisis team	Severity High+

3. Registers

Supporting working files: Enterprise Risk Register and Incident Register (XLSX). Use the Assurance Map below to track coverage.

Assurance map (template)

Top risk	1st-line control	2nd-line oversight	3rd-line assurance	Gap?
FX risk	Hedging policy	Treasury risk review	Treasury audit	No
Cyber	Security controls	Cyber risk monitoring	Cyber audit (planned)	Yes
Fraud	Anti-fraud controls	Fraud monitoring	Forensic review	No

4. Checklists

Governance health checklist

- Board and committee risk mandates documented
- Three lines clearly delineated with no gaps/overlaps
- Delegated authorities and escalation paths defined
- Risk policy hierarchy complete and current
- Assurance activities mapped and coordinated
- Committee composition and cadence appropriate
- Conflicts of interest managed
- Governance reporting reaches the board

Governance Structure

Risk is governed through three lines of defence under board oversight:

Layer	Role	Responsibility
Board	Oversight	Approves policy, appetite; oversees the risk profile
Risk / Audit Committee	Focused oversight	Reviews top risks, appetite, assurance
1st line — Management/owners	Own & manage	Identify, assess, control and report risk in operations
2nd line — Risk/Compliance	Oversee & challenge	Set framework, monitor, challenge, aggregate reporting
3rd line — Internal Audit	Assure	Independent assurance over the risk and control system

Reporting Templates

Standard governance report structure

- Executive summary & key messages
- Profile vs appetite (RAG)
- Top risks & movement
- KRIs and breaches
- Incidents & losses in period
- Actions & overdue items
- Decisions / escalations sought

KRI reporting table (example)

KRI	Current	Threshold	RAG	Trend	Action
Assurance coverage of top risks	92%	100%	Amber	Up	Plan cyber audit
Overdue board actions	1	0	Amber	Stable	Close out
Policy review currency	100%	100%	Green	Stable	Maintain

Board Reporting Example

Illustrative one-page board summary (replace with live data):

Item	Status	Commentary
Governance effectiveness	Green	Three-lines operating; charters current

Assurance coverage	Amber	One top risk (cyber) lacks independent assurance — audit planned
Escalations	Green	No unresolved escalations this period
Decisions sought	—	Approve updated Risk Committee charter

Disclaimer

This toolkit is a professional management resource, not legal, regulatory or audit advice. Calibrate scoring scales, appetite, limits and governance to your organisation, sector and applicable regulation. Sector-specific requirements (e.g. prudential, data-protection, HSE) must be confirmed against current local regulation.