OUTLIERS RISK MANAGEMENT CENTRE™

Risk Appetite Toolkit™

Design and operate risk appetite, tolerances and limits

Board / CRO / CFO · Access Tier T2 · Flagship Edition 2026

Publication-ready resource for the Outliers Resource Library

1. Full Guide

Risk appetite is the amount and type of risk an organisation is willing to take to pursue its objectives. This toolkit translates strategy into a qualitative appetite statement, cascades it into quantitative tolerances and limits, links them to KRIs, and defines what happens on a breach.

The appetite cascade

1. Strategy & objectives
2. Qualitative appetite statement (by risk type)
3. Quantitative tolerances & limits
4. KRIs that measure utilisation
5. Breach & escalation actions

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 appetite statement (template, by risk type)

Risk type	Appetite statement	Tolerance / limit	KRI
Liquidity	We maintain strong liquidity at all times	Days cash ≥ 60	Days cash on hand
Credit	We have limited tolerance for concentration	Largest counterparty ≤ 20%	Concentration %
FX/Market	We hedge material FX exposure	FX cover ≥ 70%	FX cover ratio
Operational	Low tolerance for control failures	Open critical issues = 0	Open critical issues
Cyber	Zero tolerance for critical vulnerabilities	Open critical vulns = 0	Open critical vulns
Compliance	Zero tolerance for breaches	Breaches = 0	Regulatory breaches
Fraud	Low tolerance for fraud loss	Fraud loss ≤ ₦10m/yr	Fraud loss YTD

2.2 Appetite dashboard

Working dashboard supplied as Risk_Appetite_Dashboard.xlsx — it auto-calculates utilisation and RAG status against each limit. Example output:

Risk type	Current	Limit	Utilisation	RAG
Liquidity	78 days	≥60	77%	Green
FX/Market	62%	≥70%	113%	Red
Cyber	1	0	Breach	Red
Fraud	₦6.5m	≤₦10m	65%	Green

3. Registers

Link appetite breaches to the Enterprise Risk Register and Incident Register. Every red/amber KRI should have a corresponding action with an owner and date.

4. Checklists

Appetite design checklist

- ☐ Appetite statement approved by the board

- ☐ Each material risk type has a tolerance/limit
- ☐ Limits are measurable and linked to a KRI
- ☐ Breach actions and escalation defined
- ☐ Appetite reconciled with strategy and plan
- ☐ Utilisation monitored and reported
- ☐ Appetite reviewed at least annually

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 appetite 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
FX cover ratio	62%	≥70%	Red	Down	Increase hedging
Days cash on hand	78	≥60	Green	Up	Maintain
Open critical vulns	1	0	Red	Down	Patch

Board Reporting Example

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

Item	Status	Commentary
Within appetite	Amber	5 of 7 risk types within appetite; FX and cyber in breach
FX/market	Red	Cover at 62% vs 70% floor — hedging being increased
Cyber	Red	1 critical vulnerability open — emergency remediation
Decisions sought	—	Approve temporary tolerance and remediation timeline

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.