OUTLIERS RISK MANAGEMENT CENTRE™

Fraud Risk Toolkit™

Prevent, detect and respond to fraud and financial crime

CFO / Internal Audit / Risk · Access Tier T2 · Flagship Edition 2026

Publication-ready resource for the Outliers Resource Library

1. Full Guide

Fraud risk is the risk of loss from internal or external fraud, bribery and corruption. This toolkit builds an anti-fraud programme across the three pillars — prevent, detect, respond — supported by a speak-up culture and governance.

The anti-fraud programme

Pillar	What it covers
Prevent	Fraud risk assessment, segregation of duties, approvals, vetting, awareness
Detect	Analytics, red-flags, reconciliations, whistleblowing channel
Respond	Investigation protocol, evidence handling, remediation, recovery

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 Fraud risk taxonomy

Scheme	Examples
Asset misappropriation	Theft, skimming, fake vendors
Procurement fraud	Collusion, kickbacks, false invoicing
Payroll fraud	Ghost workers, inflated claims
Financial statement fraud	Manipulated reporting
Bribery & corruption	Improper inducements
Cyber-enabled fraud	BEC, phishing, account takeover

2.2 Fraud risk register (structure + sample)

Working register: Fraud_Risk_Register.xlsx. Sample:

ID	Scheme	Risk	Score	Rating	Key control
FR-001	Procurement	Inflated invoices via collusion	12	High	3-way match + analytics
FR-002	Cyber-enabled	BEC diverts payment	15	Critical	Mandatory call-back
FR-003	Payroll	Ghost workers	6	Medium	Payroll audit + biometrics

2.3 Whistleblowing policy (core clauses)

- Confidential, multi-channel reporting (incl. anonymous)
- Non-retaliation guarantee
- Triage, investigation and feedback process
- Independence of the investigation function
- Reporting of trends to the Audit Committee

3. Registers

Pair the Fraud Risk Register with the Incident Register and Loss Event Register (XLSX) to track suspected/actual fraud events and quantify losses.

4. Checklists

Anti-fraud controls checklist

- ☐ Fraud risk assessment performed and refreshed
- ☐ Segregation of duties over payments and vendor master
- ☐ Three-way match and approval thresholds
- ☐ Mandatory call-back for payment changes
- ☐ Vendor and employee vetting
- ☐ Whistleblowing channel live and promoted
- ☐ Detection analytics / red-flag monitoring
- ☐ Investigation protocol and forensic readiness
- ☐ Fraud awareness training delivered

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 fraud 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
Fraud loss YTD (₦m)	6.5	≤10	Amber	Up	Strengthen controls
Open red-flags	2	0	Amber	Stable	Investigate
Whistleblowing cases open	1	—	Green	Stable	Progress case

Board Reporting Example

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

Item	Status	Commentary
Fraud exposure	Amber	One material BEC attempt blocked;

		controls tightened
Losses YTD	**Amber**	₦6.5m vs ₦10m tolerance
Speak-up health	**Green**	Channel active; cases handled within SLA
Decisions sought	—	Approve investment in transaction analytics

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.