NESTOR ADVISORY

Operational Risk Module

Operational Risk

Assessment Report

PREPARED FOR

Institution X

Tier 2 · Regulated, deposit-taking financial institution · Sub-Saharan Africa

SAMPLE REPORT · Institution identifiers anonymised. Methodology and structure are representative of the deliverable provided to paying clients.

Walter Tukahiirwa, CFA, ACCA · Nestor Advisory · www.nestoradvisory.com · Kampala · 2 June 2026

Executive summary

Institution X is a Tier 2, regulated, deposit-taking financial institution. The Operational Risk module scores 36.5 of 65 possible points (56%) against the Tier 2 benchmark - placing it in the Amber band: emerging, with material gaps in core risk management vocabulary.

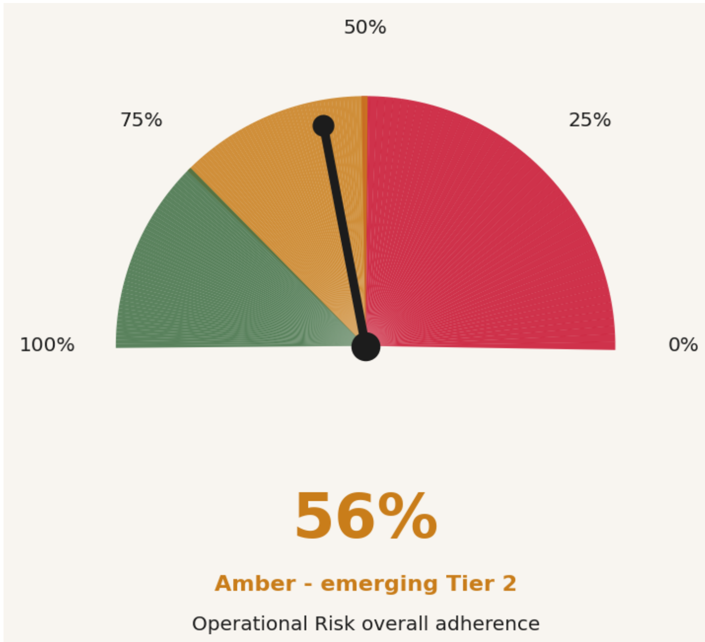

Figure 1. Operational Risk overall adherence against Tier 2 expectations.

The picture across the five operational risk families is uneven. Systems Risk is the strongest area (formal policy, mapping, daily backups, generator, user access, virus checking, EDP audit). Processes Risk is the weakest - the institution has built no Risk and Control Self-Assessment, no Key Risk Indicator dashboard, no incident reporting system. Legal and Compliance Risk follows: the assessor specifically flagged complaint handling as a 'significant' gap, and AML policy is absent.

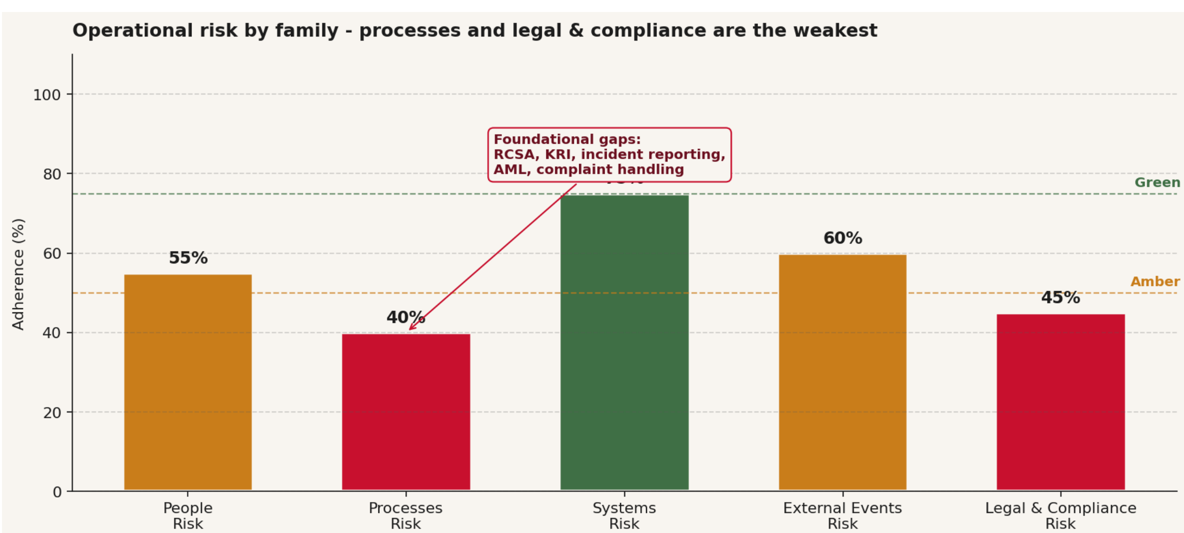

Figure 2. Adherence by operational risk family.

Top strengths

- Systems: formal IT policy, mapping of system risks, daily backups, generator, user access per individual person, virus checking, biennial Electronic Data Process audit.
- Cash management: limits on maximum cash at branches (safes and vaults), security measures including safes, vaults and armoured cash transfers.
- Reconciliation of transactions and accounts; monitoring of suspense accounts; risk tracking for internal and external reporting; checking compliance with management controls.
- Legal charter (inventory of applicable legislation including tax laws) and code of ethical conduct.

Top gaps

- No Risk and Control Self-Assessment process. No Key Risk Indicator dashboard. No incident reporting system. These are the core operational risk management artefacts a Tier 2 institution is expected to operate.
- Anti-Money Laundering policy absent; complaint handling flagged by the assessor as a significant issue rather than a partial one.
- Operational risk mapping (people, processes, external events, legal & compliance) absent or partial across four of five risk families.
- Uninterruptible Power Supply (UPS) not in place; UPS / generator testing not performed; building evacuation drills not performed.
- Communication weaknesses across the organisation noted by the assessor; changes to staff incentives not communicated; staff not aware of products.

Three urgent actions to start within the next 90 days

1. Issue an AML Policy and complaint handling protocol. Both have direct regulatory and reputational implications at the institution's current scale and deposit-taking status. 2. Stand up a Risk and Control Self-Assessment process and a Key Risk Indicator dashboard for the four most critical processes (cash handling, credit origination, deposit servicing, branch operations). 3. Implement a formal incident reporting system with a historical loss database and a lessons-learned loop into the policy review cycle.

Approach

This report applies the Nestor Advisory Risk Maturity Framework. The framework organises risk management into three tiers reflecting institutional maturity. The Operational Risk pillar covers five risk families: People, Processes, Systems, External Events and Legal & Compliance. Each is assessed across four control dimensions: Policies, Limits, Risk management tools and Risk monitoring tools.

Scoring scale

Each requirement is rated Adheres (1.0), Partially adheres (0.5), Doesn't adhere (0.0) or Not applicable (excluded from the denominator). RAG bands: Green at or above 75% (mature), Amber 50 to 74% (emerging with gaps), Red below 50% (foundational gaps).

Institution X - five-year context

Indicator	2020	2021	2022	2023	2024	Change
Total assets (USD m)	10	15	20	26	30	+200%
Active clients ('000)	33	45	63	70	78	+136%
Branches	10	13	16	21	25	+150%
Staff	102	130	145	178	201	+97%
Credit products	5	6	8	12	15	+200%

The relevant scale variables for operational risk are headcount, branches and product breadth. Staff have doubled. Branches have increased two and a half times. Credit products have tripled. Each of these multiplies the surface area on which operational risk arises - and increases the value of a structured operational risk discipline (RCSA, KRIs, incident reporting) that the institution has not yet built.

Scale grew. Operational risk vocabulary did not.

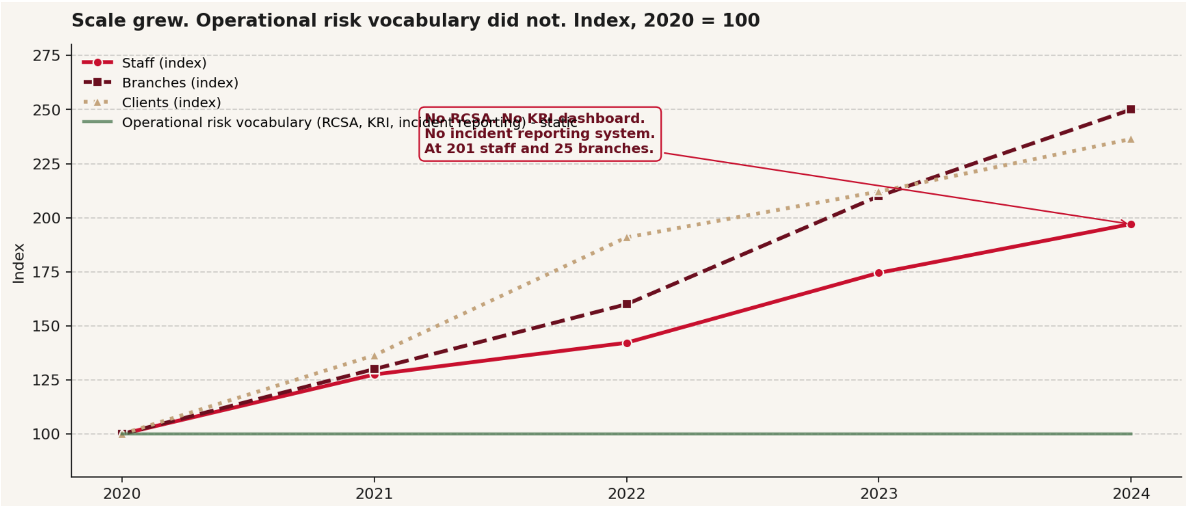

Figure 3. Operational scale indexed against the (static) state of operational risk vocabulary in the institution.

Across 2020 to 2024 the institution's staff have doubled, branches have grown two and a half times, and clients have grown 2.4 times. The operational risk management vocabulary - Risk and Control Self-Assessment, Key Risk Indicator monitoring, incident reporting - has not been built during the same period.

Why this matters at 201 staff and 25 branches

Operational risk does not scale linearly with size. As headcount and branch count grow, the number of operational error pathways grows faster. RCSA, KRIs and incident reporting are the disciplines that convert a growing operational surface area into a manageable one. Their absence is the highest-leverage gap in this assessment.

Two assessor notes that deserve direct attention

- 'Many indicators of poor communication across the organisation.' This is rare in self-assessment commentary. It is consistent with the related gaps on authorisation matrices, the absence of a structured product approval rollout (staff not aware of products) and the disconnect between incentive scheme changes and staff awareness.
- Complaint handling rated by the assessor as a 'significant issue' and judged not to be a 'partially adheres'. At a deposit-taking institution with 78,000 active clients, a weak complaint handling process is both a regulatory exposure and a reputational one.

Findings - People Risk

Policies

A formal people-risk policy is in place. The transparent remuneration sub-policy is partial; the assessor flagged that changes to the incentive scheme are not communicated to staff.

Risk management tools

In place

- Periodic training of staff on relevant policies and procedures.
- Periodic testing of personnel's knowledge of relevant policy manuals.

Material gaps

- People risk mapping (biennial) is not performed.
- Dual controls of relevant processes are partially documented.
- Job descriptions are partial.
- Risk awareness training for new staff partially in place; lessons-learned not yet systematically shared.
- Structured communication lines are partially in place. The assessor noted 'many indicators of poor communication across the organisation'.
- Authorisation matrices are not in place.

Risk monitoring tools

Quarterly analysis of variations in operating expenses is in place. Periodic staff satisfaction review and individual objective-setting in accordance with the strategy and risk framework are Tier 1-leaning items and not yet established.

Findings - Processes Risk

Processes Risk is the weakest operational risk family in the assessment. The foundational operational risk artefacts are missing.

Policies

Area	Current state
Cash transactions and handling policy	In place (policy/manual clarity needs improvement)
Use of insurance policy	In place
Risk-tracking policy	Not in place
Incident reporting policy	Not in place
Risk Self-Assessment policy	Not in place
Key Risk Indicator policy	Not in place

The vocabulary gap

Four of the six process risk policies are absent: Risk-tracking, Incident reporting, Risk Self-Assessment and Key Risk Indicators. These are not optional 'good practice' artefacts at Tier 2 - they are the language in which a modern risk function speaks. Their absence makes it structurally difficult to discover, classify and learn from operational events.

Risk management tools

Strengths: reconciliation of transactions and accounts; insurance for key assets (partial). Material gaps: process risk mapping is not performed; Business Continuity Plan partial (backup testing in place; building evacuation drills and call tree not in place); asset register limited to motorcycles only; security at branches partial (fire, theft, access controls partial); product approval and review process partial (assessor: 'staff are not aware of products'); key controls embedded in business partial; Risk and Control Self-Assessment process is not in place.

Risk monitoring tools

Suspense account monitoring, risk tracking for internal and external reporting, and compliance with management controls are in place. Dormant account monitoring is not in place (no underlying policy). Key Risk Indicator dashboard is not in place. Incident reporting is not in place.

Findings - Systems Risk

What good looks like

Formal systems policy, biennial systems risk mapping, daily backups, generator, user access per individual person, integrated loans/savings and accounting modules (with partial integration of other aspects), virus checking and biennial Electronic Data Process audit are all in place.

Remaining gaps

- Information systems integration is partial; the assessor noted that data integrity issues still remain. Data integrity is the precondition for every other system-level control.
- Quarterly checking of authorisation matrices is not performed - the same authorisation matrix gap appears in People Risk.
- Uninterruptible Power Supply (UPS) is not in place. Generator is in place but a UPS is the bridge that prevents intra-second outages affecting branch operations.
- Branches connected online or in real time only partially. Real-time connection is the precondition for most exception-based monitoring controls.
- Tier 1-leaning items not yet established: ethical hacking, network encryption, audit trails, separated dev/test/training/production environments, automated controls, ITIL processes, stress-testing, exception reporting checks. The Tier 2 institution should select two or three of these to introduce in the next 12 to 24 months.

Findings - External Events Risk

Policies and limits

Security policy is in place; Business Continuity Plan policy is in place. Outsourcing policy is not in place. Crisis management policy (Tier 1-leaning) is not yet established. Cash limits in safes and vaults are formally set.

Risk management and monitoring tools

Strengths: security measures at each branch include safes and vaults; cash transfers in armoured vehicles; backup testing is performed.

Material gaps: external events risk mapping is not performed; Business Continuity Plan strategy is not formally in place; building evacuation drills and UPS / generator testing are not performed; outsourcing monitoring, BCP testing and transaction monitoring are Tier 1-leaning items and not yet in place.

Findings - Legal & Compliance Risk

Policies

Legal charter (inventory of applicable legislation including tax laws) is in place. Code of ethical conduct is in place. These are foundational strengths.

Two material policy gaps

Complaint handling: assessor judged this 'significant' and not merely partial. AML policy: not in place. At a deposit-taking, regulated institution, both items are first-order regulatory exposures.

Whistleblower policy and suspicious transactions policy are Tier 1-leaning items not yet in place.

Risk monitoring tools

Quarterly reports of legal and compliance risk are produced. Mapping of legal and compliance risks (biennial) is not performed. Financial Action Task Force list-checking is not performed - tightly coupled to the AML policy gap. Transaction monitoring (AML) is a Tier 1-leaning item not yet in place.

Scoring summary

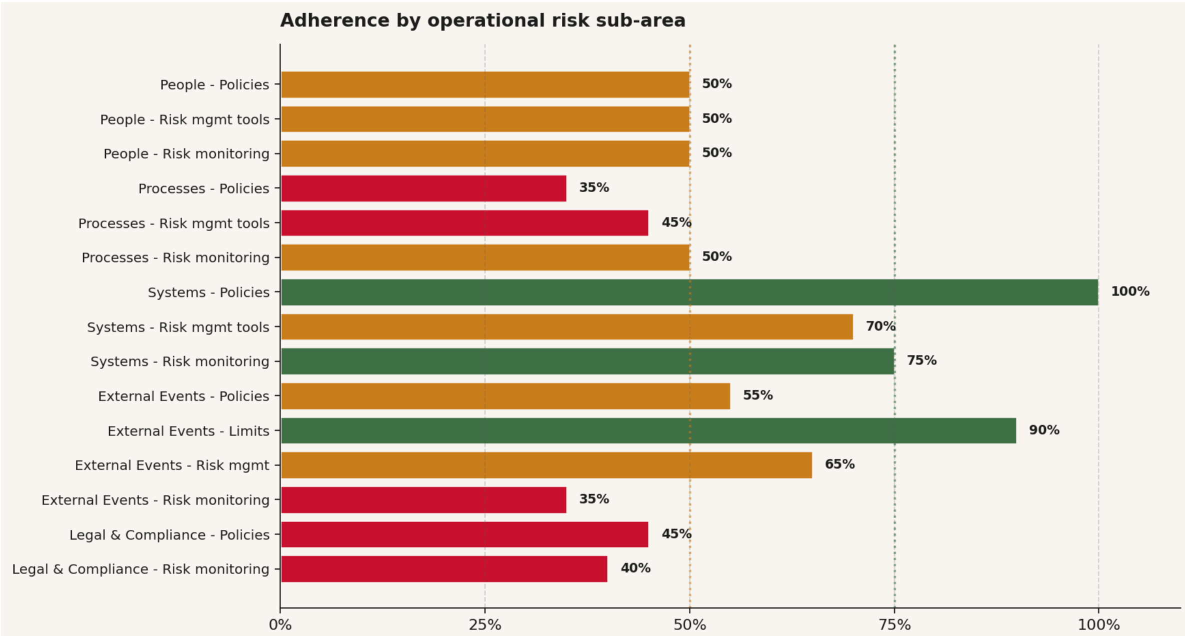

Figure 4. Adherence by operational risk sub-area.

The shape of the heat map is consistent: Systems is the only family with green sub-areas. Processes Risk is uniformly weak across policies, risk management and monitoring. Legal & Compliance is similarly weak across both dimensions. The action plan is structured to address the foundational policy gaps first, then the analytical and monitoring artefacts.

Prioritised action plan

Urgent (within 90 days)

#	Action	Verifiable indicator
U1	Issue an Anti-Money Laundering Policy and a Complaint Handling Protocol. Establish FATF list-checking at on-boarding and transaction-trigger points.	Policies approved; first month of complaint handling and FATF check logs produced.
U2	Stand up a Risk and Control Self-Assessment (RCSA) process. Start with the four highest-impact processes: cash handling, credit origination, deposit servicing and branch operations.	RCSA workshops complete; first RCSA results table presented to the board risk committee.
U3	Stand up a Key Risk Indicator dashboard for the same four processes. Include early-warning signals for fraud.	KRI dashboard in production; first issue reviewed at the risk committee.
U4	Implement a formal incident reporting system with a historical loss database and lessons-learned loop into the policy review cycle.	Incident reporting tool live; first incident report and lessons-learned summary produced.

Short-term (3 to 12 months)

#	Action	Verifiable indicator
S1	Build the operational risk vocabulary across the remaining policy gaps: Risk-tracking policy, Outsourcing policy.	Policies approved; embedded in the operational risk handbook.
S2	Complete the Business Continuity Plan: add building evacuation drills, call tree, BCP testing and a formal BCP strategy. Install UPS and add UPS / generator testing.	BCP fully operational; UPS in place; testing logs maintained.
S3	Strengthen people-risk practice: authorisation matrices in place; structured communication lines documented; remuneration changes communicated formally to all staff; job descriptions completed for all positions.	Authorisation matrices live; HR communication log; complete JD library.
S4	Begin biennial operational risk mapping cycles across People, Processes, External Events and Legal & Compliance.	Calendar documented; first formal mapping exercises completed.
S5	Resolve data integrity issues in the integrated information systems. Add quarterly authorisation	Data integrity remediation report; quarterly authorisation matrix check results; real-time branch

	matrix check. Move branches to fully real-time connection.	coverage at 100%.

Medium-term (12 to 24 months)

#	Action	Verifiable indicator
M1	Introduce two to three Tier 1-leaning systems controls: ethical hacking exercises, network encryption and segregated dev/test/production environments.	First ethical hacking exercise complete; encryption deployed.
M2	Issue a Whistleblower Policy and a Suspicious Transactions Reporting framework with transaction monitoring.	Policies approved; whistleblower channel live.
M3	Introduce annual scenario analysis and a formal tender process for purchases.	First scenario analysis report; documented tender process.

How this report is used

The Operational Risk Module is one of three paid modules in the Nestor Advisory Risk Diagnostic. The deliverable shown here represents the standard scope:

- Scored assessment against the Tier 2 (or Tier 1 / Tier 3) benchmark in the Nestor Advisory Risk Maturity Framework.
- Findings narrative across the five operational risk families, with explicit linkage between gaps observed and the institution's scale dynamics.
- Heat map and visual diagnostic for board, risk committee or executive committee consumption.
- Prioritised action plan structured into urgent, short-term and medium-term tiers, each with verifiable indicators.
- 60-minute review call with Walter Tukahiirwa, CFA, ACCA - included in the module fee.

Sector-specific tailoring (retail bank, fintech, asset finance company, SACCO, MFI, DFI) is added in real engagements.

- END OF SAMPLE REPORT -

To request a real assessment for your institution, visit www.nestoradvisory.com or contact Walter Tukahiirwa at tukahiirwaw@gmail.com.