NESTOR ADVISORY

Credit Risk Module

Credit 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 that has nearly tripled in scale over the last five years. Credit transaction-level practice is broadly in place; portfolio-level controls have not kept pace with the growth of the book.

The institution scores 39 of 73 possible points (53%) against the Tier 2 Credit Risk benchmark - the Amber band: emerging, with foundational gaps that are not yet resolved.

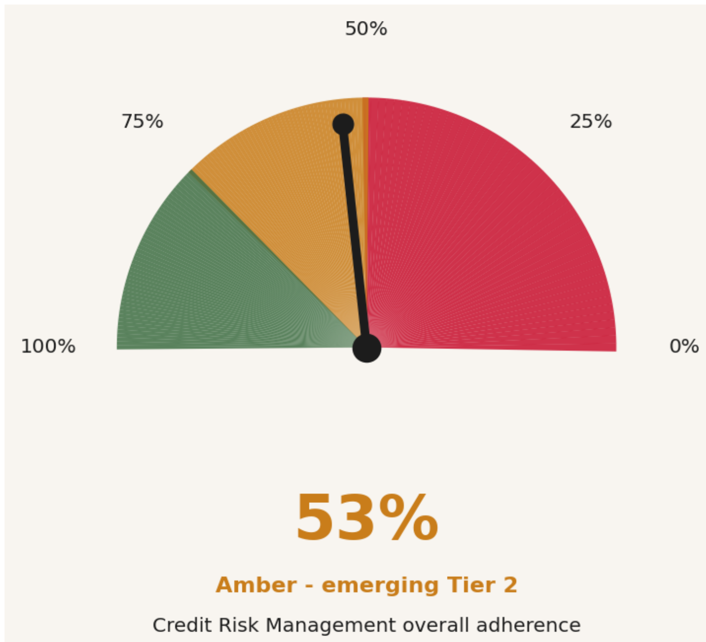

Figure 1. Credit Risk overall adherence against Tier 2 expectations.

Top strengths

- Credit policies cover the core operational areas (credit process, KYC, repayment capacity, monitoring, collection, provisioning, write-offs, approvals, code of conduct).
- Standardised application of credit policies across the network and well-functioning central and local credit committees.
- Daily arrears reports reach field staff; monthly provisioning is tooled and segmented by risk category.
- Annual geographical concentration analysis in place.

Top gaps

- No policy or limit for related-party loans; no formal loan restructuring policy.
- No portfolio diversification policy; no portfolio risk mapping.
- No portfolio concentration or PAR limits by product, branch or sector - despite credit products growing from 5 to 15 and branches from 10 to 25 over the period.
- Monthly credit and provisions reports lack trend analysis and comparison to limits.
- Field appraisal covers client OR guarantor (not both); incentives skewed to SME loans with no balancing social objectives.

Three urgent actions to start within the next 90 days

1. Approve a Portfolio Diversification Policy with concentration limits by product, branch and economic sector. 2. Issue a Related-Party Loans Policy with single-name and aggregate limits and quarterly board reporting. 3. Upgrade the monthly Credit Risk Report to include trend analysis, restructured portfolio share and explicit comparison of each indicator to its limit.

Approach

This report applies the Nestor Advisory Risk Maturity Framework, a structured benchmark for risk management practice in financial institutions. The framework organises risk management into three tiers reflecting institutional maturity, and assesses each tier across two risk families inside the Credit Risk pillar - Credit Transaction Risk and Portfolio Risk - and four control dimensions for each family: Policies, Limits, Risk management tools and Risk monitoring tools.

Tier classification

Institution X is classified Tier 2 on the basis of size (USD 5 - 50 million in assets), regulatory status (regulated, deposit-taking), audit history (audited for at least three years), rating history (rated within the last two years) and profitability (positive return on assets in at least two of the last three years).

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). Aggregate scores translate into RAG bands: Green at or above 75% (mature practice), Amber 50 to 74% (emerging practice with material gaps), Red below 50% (foundational gaps requiring priority attention).

Institution X - five-year context

Institution X is a regulated deposit-taking financial institution operating in sub-Saharan Africa. The five-year window of this assessment covers 2020 through 2024.

Indicator	2020	2021	2022	2023	2024	Change
Total assets (USD m)	10	15	20	26	30	+200%
Gross loan portfolio (USD m)	9	12	18	23	27	+200%
Active clients ('000)	33	45	63	70	78	+136%
Branches	10	13	16	21	25	+150%
Credit products	5	6	8	12	15	+200%
PAR > 30	0.25%	0.60%	0.81%	1.00%	0.40%	-
Annual write-offs ($'000)	30	100	200	300	350	+1067%
Return on assets	+2.0%	+4.4%	+3.2%	-3.0%	+0.5%	-

The 2023 stress event explained

The 2023 financial year is a clear inflection point. Portfolio at Risk over 30 days peaked at 1.0%. Return on assets fell to -3.0% - the only negative year in the period. Write-offs were ten times their 2020 level. Recovery in 2024 was modest: ROA returned to a marginal +0.5%, well below the 2021 peak of +4.4%.

Figure 2. PAR>30 and ROA, 2020 to 2024. The 2023 episode is highlighted.

Many Tier 2 institutions of this profile present the same pattern: credible transaction-level credit tools, rapid growth from a sound base, an unexpected asset quality shock in year four or five. The pattern is not random. It is the direct consequence of growth in scale outpacing growth in portfolio risk control.

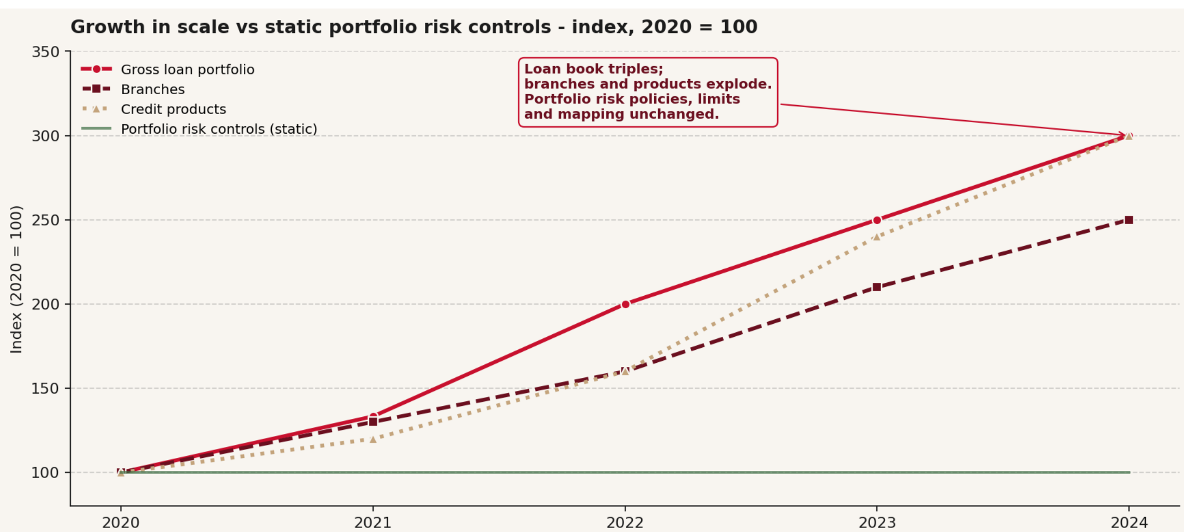

Figure 3. Growth in scale (loan book, branches, products) indexed against the static state of portfolio risk controls.

Three structural gaps explain why the 2023 deterioration was not caught earlier:

- No portfolio concentration limits by product or sector. As products grew from 5 to 15, no limit triggered escalation when a single product grew faster than the rest of the book.
- No restructured portfolio policy or limit. When clients began to struggle in late 2022, restructured loans absorbed early signals of distress without flowing into PAR or the monthly report.

- Monthly credit risk and provisions reports without trend analysis or comparison to limits. Management was looking at the right indicators but not at their direction of travel or at the line they were approaching.

The consulting insight

Institutions that complete the build of portfolio risk controls before the next growth cycle materially reduce the probability of a 2023-style episode. Institutions that do not, repeat it. The build-out is structural rather than operationally complex: it requires board sponsorship, a diversification policy, a limits framework and an analytics upgrade on existing monitoring artefacts.

Findings - Credit Transaction Risk

Policies

Credit policies cover the operationally critical areas. Two areas are absent and one is incomplete.

In place

Credit process; KYC and client visits; data verification; products and services; credit bureau use; parallel loans (external and internal); repayment capacity and over-indebtedness prevention; guarantees and valuation; loan monitoring, recovery and collection; loan provisioning; write-offs; non-permitted lending; credit approval committees; code of ethical conduct.

Material gaps

Area	Current state	Tier 2 expectation
Related-party loans	Not covered	Documented policy with single and aggregate limits and board reporting
Loan restructuring	Not covered	Policy with separate approval committee, MIS tagging, ageing reset rules
Client protection alignment	Partially aligned	Credit policies fully aligned with recognised client protection principles

Limits

Limits exist in pockets - on write-offs, on provisions over PAR30, and by loan risk category - but the framework as a whole is fragmented. Targets exist where the benchmark expects board-approved limits with explicit escalation. Specifically, there are no limits on PAR by ageing structure, on restructured portfolio share, or on related-party loans.

Why this matters

A target is a goal. A limit is a tripwire - when it is hit, defined people must take defined action. The absence of formal PAR limits by ageing meant that, through 2022 and 2023, deteriorating ageing was visible but no trigger forced the response.

Risk management tools

Strong on tooling (standardised credit policy application, sector knowledge, credit bureau consultation, repayment capacity tool, well-functioning credit committees, monthly provisioning by risk category, separate approval committee for restructured loans). Three material gaps:

Area	Current state	Tier 2 expectation
Field visits	Client OR guarantor	Systematic visit to BOTH client and guarantor

Incentive system	Skewed to SME loans; no social-objective measures	Incentives aligned with both financial and social objectives
Guarantee evaluation	Internal tool exists but inconsistently applied	Consistent application with periodic independent re-valuation for higher-value collateral

Risk monitoring tools

Daily arrears reports reach field staff. The monthly credit risk report exists and is reviewed, but the analytics layer is thin: PAR by ageing structure, restructured portfolio share, trend analysis and comparison to limits are missing. Monthly provisions monitoring covers provisions over PAR30 and by risk category but omits trend analysis, limits comparison and the provision expense ratio. There is no monthly report of related-party loans. Mapping of credit transaction risks is partial rather than systematic. More advanced tools - statistical scoring, vintage analysis, portfolio transition analysis - are absent (Tier 1-leaning).

Findings - Portfolio Risk

Portfolio risk is the risk that the loan book in aggregate is too concentrated, too undiversified or too exposed to a single sector, geography, methodology or product. For Institution X this is the weakest area of the assessment.

Policies

There is no formal portfolio diversification policy.

Why this matters

Without a diversification policy, growth decisions on new products, new branches and new sectors are made at the operational level without a strategic frame. Each individual decision can be defensible. The aggregate effect over five years can be a portfolio that is materially more concentrated than the board would consciously sanction.

Limits

A single limit exists - the maximum loan amount per credit product. This is necessary but not sufficient. The benchmark expects portfolio concentration limits and PAR limits across multiple dimensions.

Dimension	Concentration limit?	PAR limit?
Product	Partial - informal	No
Branch	No	No
Economic sector	Segmented but no limit	No
Credit methodology	Not assessed	Not assessed
Region	Not assessed	Not assessed

Risk management and monitoring tools

Annual analysis of geographical areas is performed. Annual analysis of economic sectors is not performed. Weekly portfolio concentration and PAR reports are produced and reach the credit team, but neither contains trend analysis or comparison to limits. Sector coverage is incomplete in both. Mapping of portfolio risks has not been performed.

Why this matters

The weekly reports are the right artefacts. Inside the reports the analytical layer that converts data into management decisions is missing. This is the single highest-leverage area for Institution X to invest in over the next two quarters - the artefacts already exist; upgrading them does not require new infrastructure.

Scoring summary

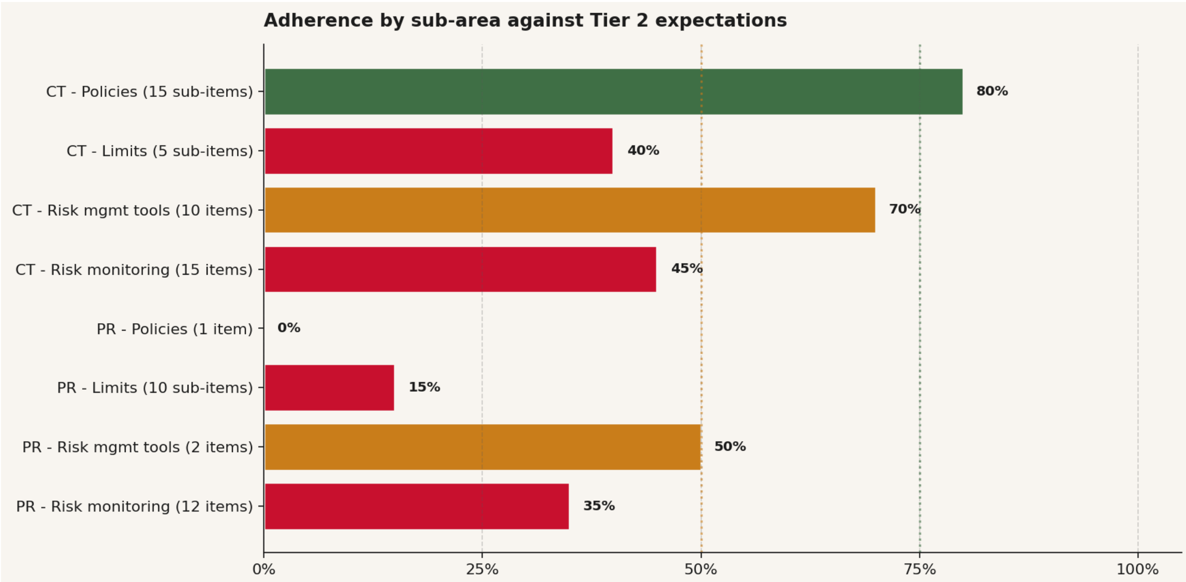

Figure 4. Adherence by sub-area against Tier 2 expectations.

The shape of the heat map is concentrated rather than balanced. Credit transaction policies are mature. Credit transaction risk management tools sit at the upper end of amber. Everything else - credit transaction limits, credit transaction risk monitoring, and the entire portfolio risk family - sits below 50%. This is not a 'balanced amber' picture. It is a transaction-strong, portfolio-weak picture. The action plan that follows is structured accordingly.

Prioritised action plan

Recommendations are sequenced into three priority tiers. Urgent addresses the structural causes of the 2023 deterioration. Short-term closes the remaining policy and limit gaps. Medium-term introduces tools that protect the institution as it continues to grow toward Tier 1.

Urgent (within 90 days)

#	Action	Verifiable indicator
U1	Issue Portfolio Diversification Policy with concentration limits and PAR limits by product, branch and sector. Board approval.	Policy document; limits embedded in MIS; first monthly board pack reflects limits.
U2	Issue Related-Party Loans Policy with single-name and aggregate limits. Quarterly board reporting and external audit attestation.	Policy approved; first RPL report at next board meeting.
U3	Issue Loan Restructuring Policy: separate approval committee, MIS tagging, ageing reset rule; restructured share in monthly report.	Policy approved; restructured share visible in next monthly credit risk report.
U4	Upgrade monthly Credit Risk Report: add PAR by ageing, restructured share, 12-month rolling trend, explicit comparison to limit.	Revised report; first issue to ALCO and board credit committee.

Short-term (3 to 12 months)

#	Action	Verifiable indicator
S1	Reinforce field appraisal: visit client AND guarantor on every appraisal. Update credit manual and loan officer training.	Updated manual; refreshed training; audit sample 90%+ compliant within 6 months.
S2	Rebalance field staff incentive scheme - add social-objective measures, reduce SME volume dominance.	Revised scheme; first quarter of payouts under new scheme.
S3	Bring credit policies fully into line with recognised client protection principles.	Self-assessment; updated credit manual.
S4	Add trend analysis, limits comparison and provision expense ratio to monthly provisions monitoring report.	Revised report; first issue circulated.
S5	Add annual analysis of economic sectors. Integrate with the new sector concentration limits.	First annual sector analysis paper presented to board credit committee.

Medium-term (12 to 24 months)

#	Action	Verifiable indicator
M1	Establish biennial credit transaction and portfolio risk mapping calendars.	Calendars documented; first formal mapping exercises completed.
M2	Introduce monthly vintage analysis; begin building a portfolio transition matrix.	Vintage report in production by month 18.
M3	Pilot a statistical credit scoring model on the two largest products.	Pilot results presented; decision to extend or refine documented.

How this report is used

The Credit 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 by sub-area, with explicit linkage between gaps observed and historical operating outcomes.
- Heat map and visual diagnostic that enables a board or executive committee to grasp the picture in two minutes.
- 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.

NESTOR ADVISORY

Asset Liability Management Module

Asset Liability Management

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 Asset Liability Management (ALM) module shows the weakest performance across the Nestor Advisory diagnostic. The institution scores 24.5 of 59 possible points (42%) against the Tier 2 ALM benchmark - the Red band: foundational gaps requiring priority attention.

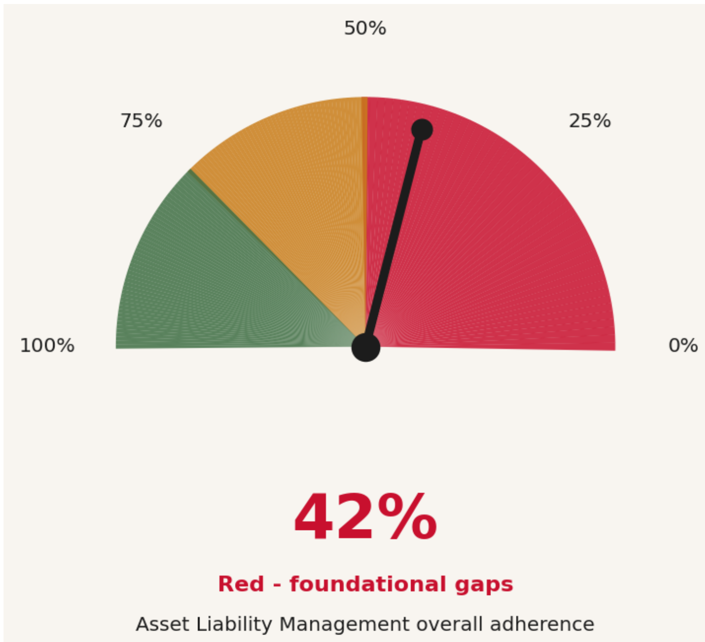

Figure 1. ALM overall adherence against Tier 2 expectations.

The picture is sharply uneven. Foreign exchange management is mature - formal policy, NOP limit, monthly volatility and quarterly exposure reporting all in place. Everything else is weak. There is no formal liquidity policy, no formal interest rate risk policy, no formal investment portfolio policy, and no internal capital adequacy limit.

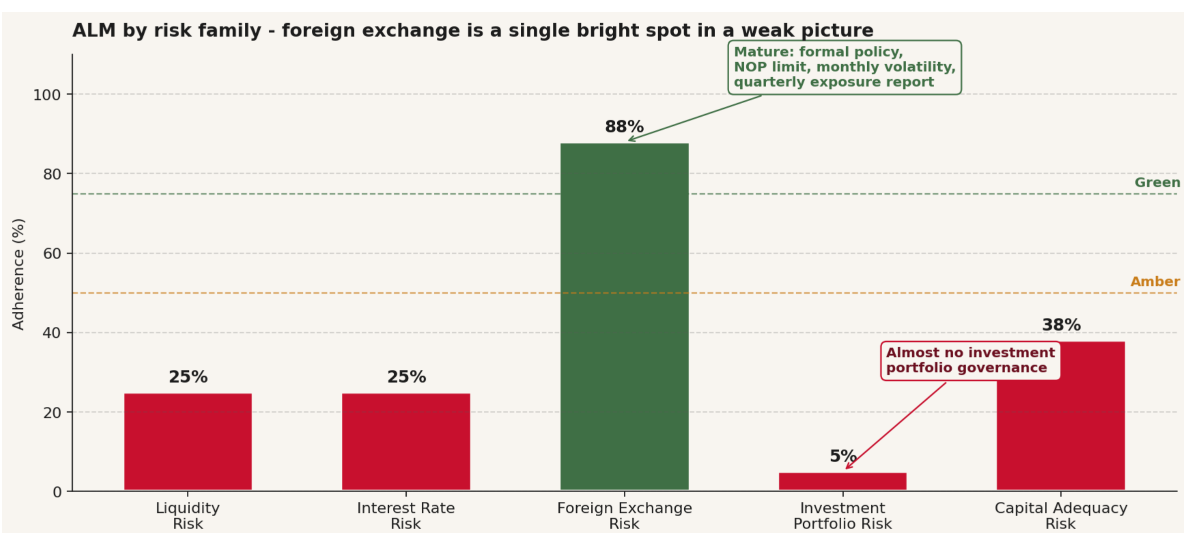

Figure 2. Adherence by ALM risk family. FX is the only family at a mature standard.

Top strengths

- Foreign exchange: formal policy in place; institution does not transfer FX risk to clients; NOP limit set; quarterly FX exposure report includes NOP, stressed sensitivity and limits comparison.
- Weekly projected cash flow report and monthly lender concentration report in production.
- Liquid investment accounts and pre-approved credit lines provide a basic liquidity buffer.
- Capital adequacy is monitored monthly with trend analysis.

Top gaps

- No formal liquidity policy; no depositor concentration limit; no liquidity contingency plan; no behavioural or dynamic liquidity modelling.
- No formal interest rate risk policy. Existing exposure limit flagged as potentially inappropriate. No repricing gap analysis. No net interest income sensitivity.
- No formal investment portfolio policy or concentration limits.
- No limit on debt-to-equity ratio or capital over risk-weighted assets - the core capital adequacy guardrail is absent.
- Funding plan owned by the CEO rather than the CFO - a structural governance flag.

Three urgent actions to start within the next 90 days

1. Approve and roll out a Liquidity Risk Policy including depositor and lender concentration limits, behavioural deposit assumptions, minimum net-liquid-asset ratios and a documented liquidity contingency plan. 2. Set an internal capital adequacy limit 200 to 400bps above the regulatory minimum, with explicit board escalation. 3. Reassign ownership of the funding plan from CEO to CFO, with a monthly funding paper to the ALCO.

Approach

This report applies the Nestor Advisory Risk Maturity Framework. The framework organises risk management into three tiers reflecting institutional maturity. The Asset Liability Management pillar covers five risk families: Liquidity, Interest Rate, Foreign Exchange, Investment Portfolio and Capital Adequacy. Each is assessed across four control dimensions - Policies, Limits, Risk management tools and Risk monitoring tools.

ALM as a discipline applies to any institution managing a balance sheet - retail banks, microfinance institutions, SACCOs, fintechs, asset finance companies and DFIs. Some items in this module specifically reference deposits; non-deposit-taking respondents mark those individually as 'Not applicable' and continue with the rest.

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%
Gross loan portfolio (USD m)	9	12	18	23	27	+200%
Active clients ('000)	33	45	63	70	78	+136%
Branches	10	13	16	21	25	+150%
PAR > 30	0.25%	0.60%	0.81%	1.00%	0.40%	-
Return on assets	+2.0%	+4.4%	+3.2%	-3.0%	+0.5%	-

Two features of the institution's profile drive the ALM assessment: deposit-taking and regulated (so liquidity controls and depositor concentration are first-order concerns), and rapid balance-sheet expansion (so capital adequacy build-back has not kept pace with asset growth, especially after the 2023 loss).

Deposit growth running ahead of ALM controls

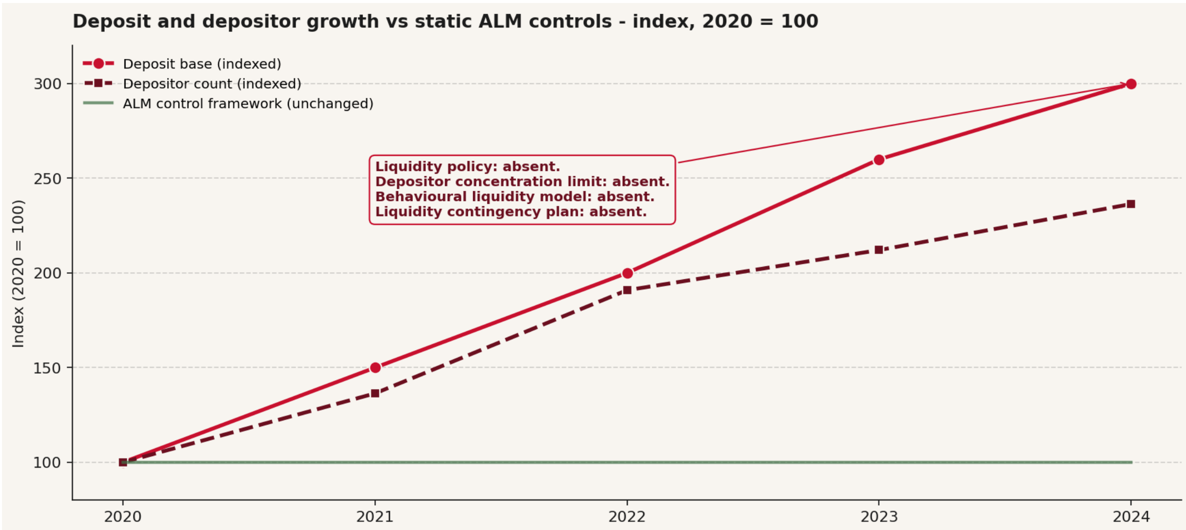

Figure 3. Deposit and depositor growth indexed against the (essentially static) ALM control framework.

Across 2020 to 2024 the deposit base has tripled. The number of depositors has more than doubled. Over the same five years the ALM control framework has not been formalised. The institution is running a 2024-size deposit book on a 2020-vintage ALM discipline.

Funding-side amplifiers of the 2023 event

With no liquidity contingency plan and no depositor concentration limit, any tightening of funding in 2023 had to be addressed reactively rather than from a pre-approved playbook. Without a behavioural liquidity report and a dynamic liquidity report, management was looking at point-in-time liquidity numbers without an understanding of how stable the underlying deposits actually were. Without an internal capital adequacy limit, the 2023 ROA loss eroded capital silently - no formal trigger forced a board conversation until prudential boundaries came uncomfortably close.

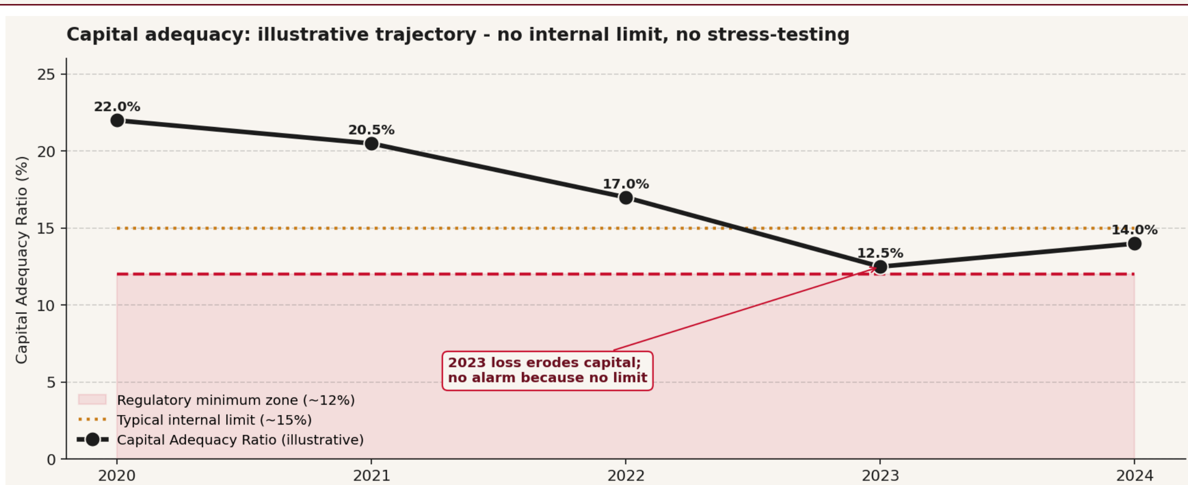

Figure 4. Illustrative capital adequacy trajectory against indicative reference lines.

Figure 4 is illustrative; actual capital adequacy ratios were not in scope of the self-assessment. The shape is consistent with the institution's reported profitability path. The structural point is that without an internal limit above the *regulatory minimum, there is no early-warning system to force a capital response before the regulatory minimum is approached.*

Findings - Liquidity Risk

Policies and limits

There is no formal liquidity policy. None of the depositor or lender concentration limits, net-liquid-asset ratios or time-band coverage limits required at Tier 2 are formally board-approved.

Requirement	Current state
Lender concentration limits	No formal per-bank limit
Depositor concentration limits	Not in place
Net liquid assets vs total assets	Not in place
Net liquid assets vs deposits up to 90 days	Not in place
Time-band coverage under behavioural / dynamic scenarios	Not in place

Risk management and monitoring tools

Liquid investment accounts and pre-approved credit lines are in place. Coherent product/funding strategies and the funding plan are partial. There is no liquidity contingency plan.

Governance flag

The funding plan currently sits with the CEO rather than the CFO. ALM practice expects the CFO (or treasurer) to own the funding plan and present it to the ALCO. CEO ownership conflates execution responsibility with oversight responsibility and dilutes the role of the ALCO.

Reporting: weekly cash flow and monthly lender concentration reports are in production; depositor concentration report, monthly behavioural liquidity report and monthly dynamic liquidity report are absent. The monthly liquidity indicators report exists but lacks trend analysis and full limits comparison.

Findings - Interest Rate Risk

No formal IRR policy. An exposure limit exists but was flagged by the assessor as potentially inappropriate - it satisfies the existence test but may not be calibrated to actual sensitivity. Limits on net interest income sensitivity and on the sensitivity of economic value of equity are absent.

What this means in practice

An exposure limit that has not been calibrated to the institution's repricing profile is a tick-the-box artefact. The likely path is to commission a repricing gap analysis, calculate net interest income sensitivity under a parallel 200bp shock, and recalibrate the limit from that empirical base.

Risk management tools: product and funding strategies for repricing mismatches are partial. No IR contingency plan; no use of derivative instruments. Monitoring: quarterly IR volatility report and quarterly exposure report (with limits comparison) are in place. Repricing gap analysis, NII sensitivity and IR stress-testing are absent.

Findings - Foreign Exchange Risk

Mature: what good looks like

Formal FX policy in place. Institution does not transfer FX risk to clients. NOP limit set. Monthly currency volatility report and quarterly FX exposure report (including NOP, stressed FX income sensitivity and limits comparison) produced. Coherent product and funding strategies avoid currency mismatches at source. Non-derivative instruments deployed for residual exposure. Biennial FX risk mapping in place.

Limited remaining gaps: stressed FX income sensitivity is reported but not yet set as a formal limit; FX contingency plan and Value-at-Risk analysis are not in place (Tier 1-leaning); quarterly FX stress-testing report not yet produced - data inputs already exist so this is a low-effort upgrade.

Findings - Investment Portfolio Risk

Investment portfolio risk arises from holdings of financial instruments and placements with other financial institutions. This family is essentially undeveloped.

Requirement	Current state
Formal investment portfolio policy (selection criteria, responsibilities)	Not in place
Concentration limits by institution and maturity	Not in place
Committee for permitted institutions, instruments and concentrations	Role of Board Finance Committee not clearly defined
Mapping and monthly investment portfolio report	Not applicable in current state (limited positions)

Why this matters

Several items are recorded 'Not applicable' because investment positions are currently small. The risk is not position size; it is the absence of any governance frame should the institution begin to hold liquid investments more actively - which Tier 2 institutions of this scale typically do. The fix is structural - issue a policy, define the committee, set concentration limits - regardless of current position size.

Findings - Capital Adequacy Risk

Dividend distribution policy is partial. Minimum percentage of profits to be capitalised is partially defined. The single most consequential gap is the absence of an internal limit on the debt-to-equity ratio or on adjusted capital over risk-weighted assets.

The internal-limit gap

Without an internal capital adequacy limit set above the regulatory minimum, the institution operates with no early-warning trigger. The 2023 ROA loss of -3.0% will have eroded capital meaningfully (Figure 4 illustrates a plausible path). The absence of internal escalation suggests there was no trigger to escalate against. A typical Tier

2 internal limit sits 200 to 400bps above the regulatory minimum, with a defined corrective action path.

Monitoring: monthly capital adequacy monitoring exists with the relevant ratio and trend analysis. Comparison to internal limits is absent (consistent with the limit gap). Capital adequacy stress-testing is not performed.

Scoring summary

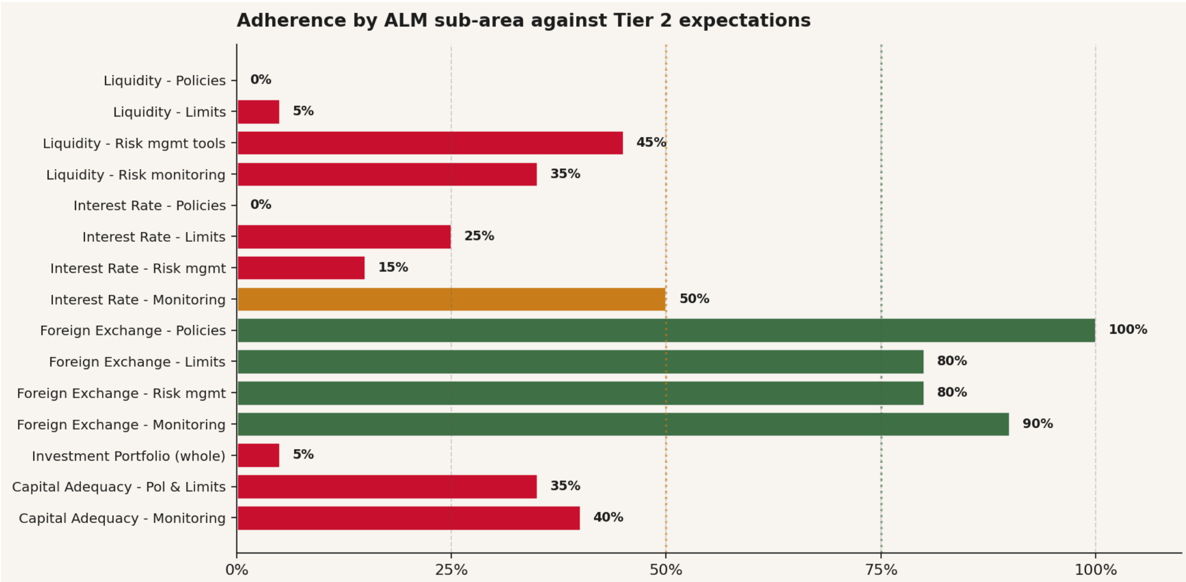

Figure 5. Adherence by ALM sub-area.

The shape of the heat map is concentrated rather than balanced. Foreign exchange risk dominates the green and amber zones. Liquidity, interest rate, investment portfolio and most of capital adequacy sit in the red zone. The action plan mirrors this concentration: urgent build-out in liquidity policy and limits and capital adequacy limits, followed by interest rate risk policy and analytics.

Prioritised action plan

Urgent (within 90 days)

#	Action	Verifiable indicator
U1	Issue formal Liquidity Risk Policy with ALCO mandate, lender and depositor concentration limits, NLA ratio limits, behavioural deposit assumptions, and a liquidity contingency plan with named triggers and actions.	Policy approved; first monthly ALCO pack uses the new framework.
U2	Set an internal capital adequacy limit (D/E or capital/RWA) 200 to 400bps above the regulatory minimum. Define breach escalation path.	Limit approved; embedded in monthly capital monitoring; comparison to limit visible in first monthly report.
U3	Reassign funding plan ownership from CEO to CFO. Monthly funding paper to ALCO from CFO.	Reassignment documented; first monthly funding paper at the ALCO.
U4	Add a monthly depositor concentration report and a monthly behavioural liquidity report.	Reports produced; reviewed at the ALCO.

Short-term (3 to 12 months)

#	Action	Verifiable indicator
S1	Issue formal IRR Policy. Commission repricing gap analysis. Calculate NII sensitivity under +/- 200bp shock. Recalibrate exposure limit.	Policy approved; repricing gap report produced; recalibrated limit in place.
S2	Issue formal Investment Portfolio Policy. Define responsible committee. Set concentration limits by institution and maturity even if positions are currently small.	Policy and committee mandate approved.
S3	Add monthly dynamic liquidity reporting and sight-deposit volatility report. Build out monthly liquidity indicators report (trend, full limits comparison).	Revised monthly liquidity pack to the ALCO.
S4	Issue formal dividend distribution policy with explicit capital preservation gates.	Policy approved.
S5	Begin biennial mapping cycles for liquidity, interest rate and investment portfolio risks.	First formal mapping exercises completed.

Medium-term (12 to 24 months)

#	Action	Verifiable indicator
M1	Introduce quarterly IR stress-testing. Move toward EVE sensitivity reporting.	First quarterly IR stress-test report.
M2	Introduce quarterly capital adequacy stress-testing.	First quarterly capital stress-test report.
M3	Add Value-at-Risk analysis to FX monitoring; quarterly FX stress-testing report; FX contingency plan.	VaR report; FX stress-test report; FX contingency plan approved.

How this report is used

The ALM 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 ALM risk families, with explicit linkage to historical operating outcomes.
- Heat map and visual diagnostic for board, ALCO 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.

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.

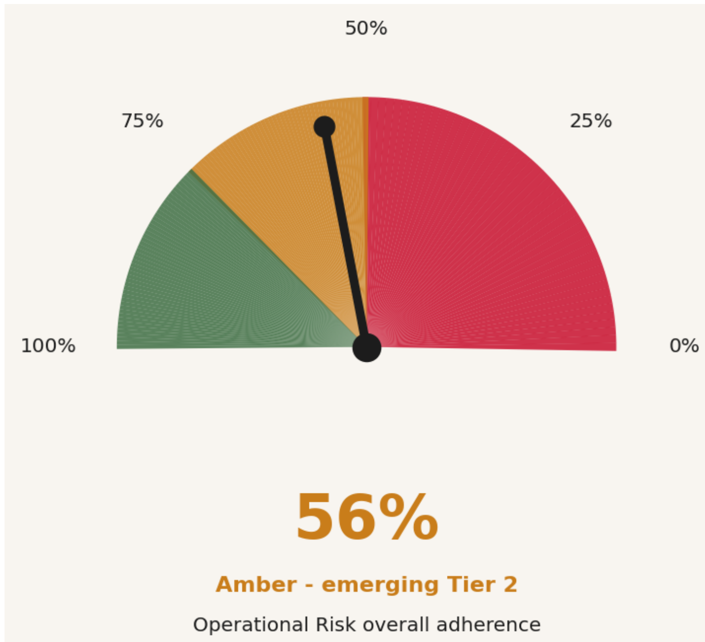

Figure 1. Operational Risk overall adherence against Tier 2 expectations.

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.

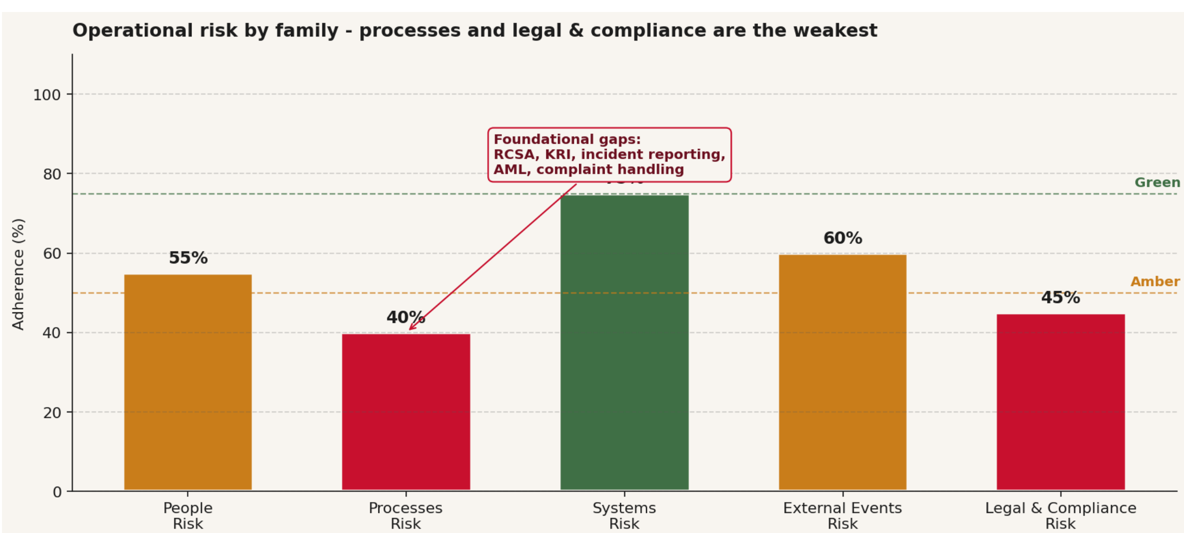

Figure 2. Adherence by operational risk family.

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.

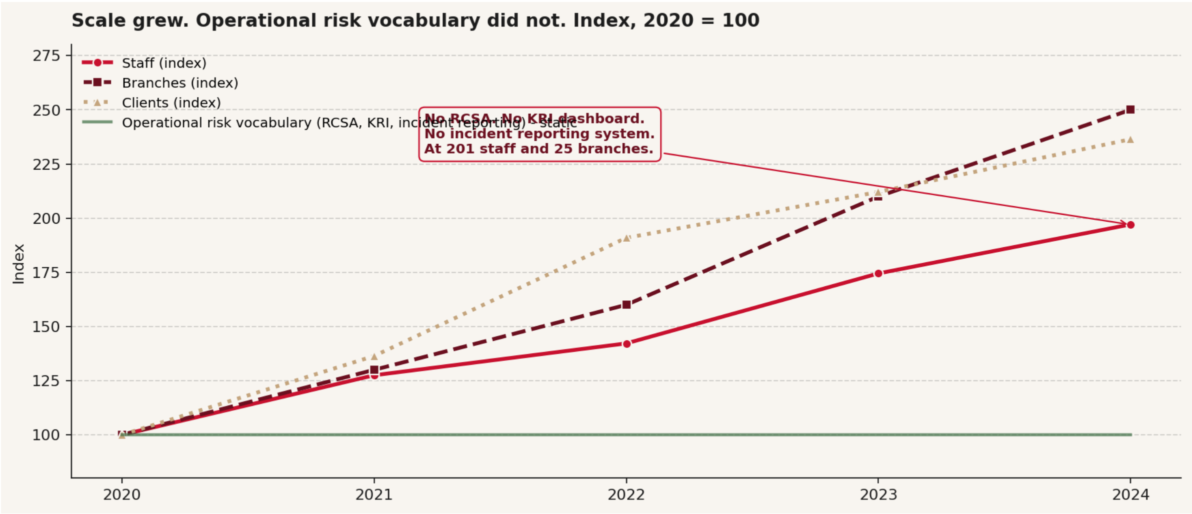

Figure 3. Operational scale indexed against the (static) state of operational risk vocabulary in the institution.

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

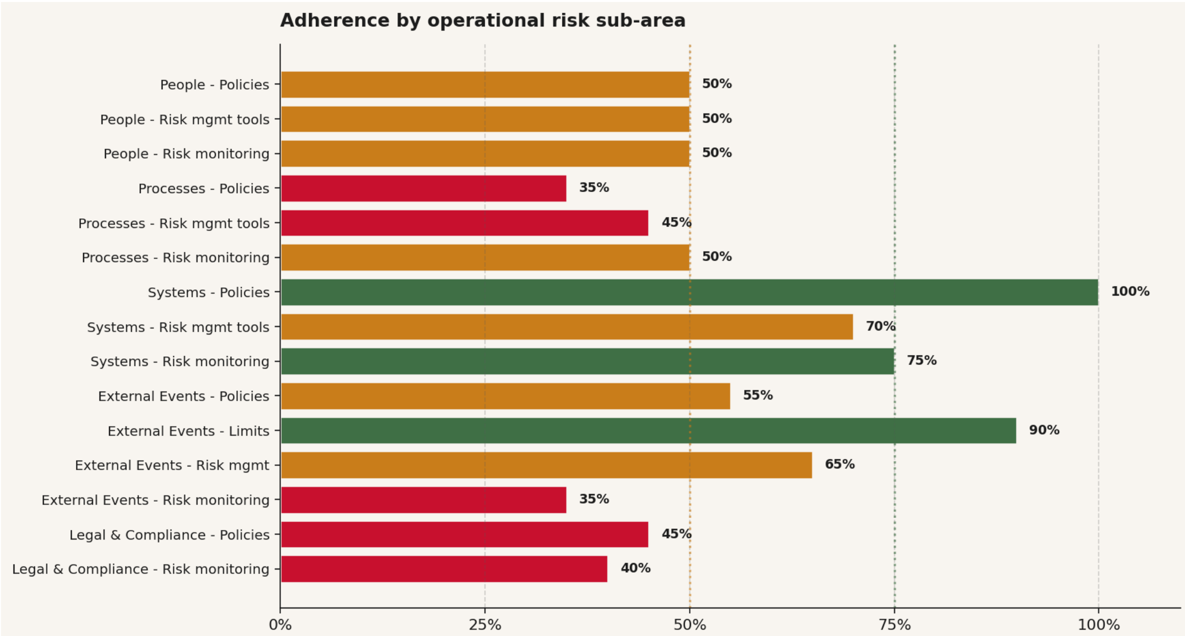

Figure 4. Adherence by operational risk sub-area.

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.