ENHANCED EDITION · 2026

Internal Control, Risk Management & Audit Readiness Toolkit

Foreword

Integrated COSO · ISO 31000 · IIA Standards · NCCG 2018

This Enhanced Edition is the integrated reference for Nigerian financial-services institutions and other regulated entities that must demonstrate, at any moment, that their control environment is designed, operated, evidenced and assured to a board-grade standard. It consolidates the original Internal Control & Audit Readiness Toolkit (the Framework & Policy Manual, the Process Narratives & Audit Readiness Guide, the Risk & Control Matrix and the readiness trackers) with the Enhancement Pack — the Enterprise Risk Management framework, Risk Appetite Statement template, the 52-indicator KRI Library, Internal Audit and Audit Committee Charters, the Fraud Risk Management Framework, the Regulatory Compliance Monitoring Framework, the Audit Committee Dashboard specification and the 180-day Implementation Roadmap.

It is aligned to the COSO Internal Control and COSO ERM (2017) frameworks, ISO 31000 and ISO/IEC 27001, the IIA Global Internal Audit Standards, the Nigerian Code of Corporate Governance 2018 and the supervisory expectations of the Central Bank of Nigeria, the Financial Reporting Council of Nigeria, the Securities and Exchange Commission, the Nigeria Data Protection Commission, PenCom, and the Nigerian Financial Intelligence Unit. Illustrative figures, owners and dates are samples to be replaced with entity-specific data before reliance.

Five reasons to adopt the Enhanced Edition

-
-
-
-
-

Outliers Professionals Ltd · Lagos · Abuja · Port Harcourt
Version 1.0 · 2026 Edition

Part 1 · Internal Control Framework & Policy Manual

1.1 Scope & Applicability

This Manual applies to all business units, support functions, subsidiaries and outsourced arrangements. It covers manual and automated controls, entity-level and process-level controls, and controls operated by third parties on the organisation's behalf. All employees, contractors and secondees who operate, review or rely on controls are bound by it.

1.2 Governance — the Three Lines Model

Line	Who	Responsibility
First line	Business & support functions	Own and operate controls day-to-day; identify and manage risks within appetite; comp
Second line	Risk, Compliance, Information Security	Set policy and methodology; monitor design and operation; challenge the first line; agg
Third line	Internal Audit	Provide independent, objective assurance to the Board and Audit Committee on the a
Oversight	Board & Audit Committee	Set tone at the top and risk appetite; oversee the control environment; review findings

1.3 Integrated Control Framework

The control environment is anchored to the five components of COSO Internal Control, aligned with the ISO/IEC 27001 information-security management standard and the Nigerian governance regime.

COSO Component	ISO/IEC 27001 Linkage	Governance Application
Control Environment	Leadership (Cl.5); competence & awareness (Cl.7); organisational controls (A.5)	Code of conduct, board oversight, delegated authority an
Risk Assessment	Risk assessment & treatment (Cl.6, Cl.8)	Enterprise risk methodology; inherent/residual rating; frau
Control Activities	Annex A controls: access, cryptography, operations, change	Key preventive and detective controls across all cycles ar
Information & Communication	Communication (Cl.7.4); logging & monitoring (A.8)	Management and regulatory reporting; escalation channe
Monitoring Activities	Performance evaluation & improvement (Cl.9, Cl.10)	Continuous monitoring, self-assessment and independen

1.4 Roles & Responsibilities

Role	Key Responsibilities
Board / Audit Committee	Approve risk appetite and key policies; oversee control effectiveness; review audit findings and
Chief Risk Officer	Own the risk and control methodology; maintain the Risk & Control Matrix; report aggregate risk
Chief Information Security Officer	Own the ISMS, Statement of Applicability and IT general controls; manage information-security
Financial Controller	Own financial-close and reporting controls; ensure reconciliations and journal controls operate.
Money Laundering Reporting Officer	Own AML/CFT, sanctions and customer due-diligence controls; file SARs.
Head of Internal Control	Maintain this Toolkit; coordinate audit readiness; track deficiencies to closure.
Internal Audit	Independently test controls and report to the Audit Committee; validate remediation.

1.5 Key Control Policies

Segregation of Duties

No single individual may control all phases of a transaction. Initiation, authorisation, custody, recording and reconciliation must be distributed so that errors and fraud cannot occur and remain undetected. Where complete segregation is impractical, compensating controls (independent review, surprise checks, system logging) must be documented and operated.

Delegation of Authority

All financial and operational decisions must be made within the Board-approved Delegation of Authority matrix. Approval limits are enforced in systems where possible and reconciled to configuration periodically. Decisions above delegated limits are escalated to the appropriate committee.

Manual Journal & Financial Reporting Controls

Manual journals above the defined threshold require independent preparer and reviewer roles, supporting evidence, and an audit trail. Balance-sheet accounts are reconciled monthly, independently reviewed and cleared on a timely basis. The general ledger period is locked after sign-off; reopening requires Financial Controller approval.

Access Management (ISO/IEC 27001 A.8)

Access to financially significant and information systems is granted on the basis of least privilege and documented approval, removed promptly on role change or termination, and recertified periodically. Privileged access is restricted, logged and monitored.

Change Management

Changes to production systems follow a documented lifecycle: request, impact assessment, testing, approval and release, with segregation between those who develop and those who deploy. Emergency changes are subject to retrospective review.

AML/CFT, Sanctions & Customer Due Diligence

The organisation operates a risk-based programme covering customer due diligence and enhanced due diligence, ongoing monitoring, real-time sanctions screening and suspicious-activity reporting. Customers are not activated until due diligence is complete and approved, and screening matches are cleared before payments are released.

Third-Party & Outsourcing Risk

Material outsourced arrangements are subject to due diligence before onboarding, risk-tiered ongoing monitoring, review of independent assurance reports (e.g. SOC reports), and contractual right-to-audit. Accountability for outsourced controls remains with the organisation.

1.6 Deficiency Management & Escalation

Severity	Definition
Material Weakness	A deficiency, or combination, that creates a reasonable possibility of a material misstatement or signific
Significant Deficiency	Less severe than a material weakness but important enough to merit attention by those responsible for
Deficiency	A control that does not allow management or staff, in the normal course of their duties, to prevent or de

Part 2 · Process Narratives & Audit Readiness

Financial Close & Reporting (FCR)

Objective. Produce accurate, complete and timely financial statements free from material misstatement.

Key process steps

- Sub-ledgers reconciled and closed; accruals and estimates prepared.
- Manual journals raised, supported and independently reviewed (FCR-01).
- Balance-sheet accounts reconciled and reviewed; open items aged and cleared (FCR-02).
- General ledger period locked after Financial Controller sign-off (FCR-03).
- Financial statements prepared, reviewed and approved.

Key controls

- Preparer/reviewer segregation on manual journals above threshold (FCR-01).
- Independent review and sign-off of monthly reconciliations (FCR-02).
- System-enforced period lock with controlled reopening (FCR-03).

Supporting systems. General ledger / ERP, reconciliation tool, consolidation system.

Evidence for audit. Journal listings with approvals, reconciliation files with review evidence, period-lock configuration, signed financial statements.

Procure-to-Pay (P2P)

Objective. Ensure payments are made only for valid, authorised goods and services to approved vendors.

Key process steps

- Vendor onboarded with due diligence; vendor master maintained.
- Purchase order raised and approved within authority limits.
- Goods/services received and matched to PO and invoice (three-way match).
- Payment run prepared, reviewed and released by two officers (P2P-02).
- Bank-detail changes verified by independent call-back (P2P-01).

Key controls

- Dual authorisation of vendor master changes; three-way match before payment (P2P-01).
- System block on duplicate invoice numbers; dual release of payment runs (P2P-02).

Supporting systems. ERP / accounts-payable module, banking platform.

Evidence for audit. Vendor change logs, matched PO/GRN/invoice samples, payment-run reports with release evidence.

Credit & Lending (CRD)

Objective. Originate and monitor credit within approved policy, appetite and provisioning requirements.

Key process steps

- Application assessed against scoring and credit policy.
- Approval within delegated limits; larger exposures escalated to Credit Committee (CRD-01).
- Facility disbursed; collateral and covenants recorded.
- Portfolio monitored; expected credit losses modelled and provisioned (CRD-02).

Key controls

- System-enforced limits and committee approval for large exposures (CRD-01).
- Governed, validated ECL model with CFO-signed provisioning (CRD-02).

Supporting systems. Loan origination system, credit risk / ECL model, collateral register.

Evidence for audit. Credit files, committee minutes, limit configuration, ECL model validation and provisioning papers.

AML/CFT, Sanctions & KYC

Objective. Detect and prevent financial crime; meet customer due-diligence and reporting obligations.

Key process steps

- Customer onboarded with risk-based CDD/EDD; activation only after approval (KYC-01).
- Real-time sanctions screening at onboarding and payment; matches cleared before release (AML-02).
- Transactions monitored; alerts investigated within SLA (AML-01).
- Suspicious activity assessed and reported by the MLRO; periodic CDD refresh tracked.

Key controls

- CDD/EDD completion and approval gate before activation (KYC-01).
- Automated transaction monitoring with timely alert disposition (AML-01).
- Real-time sanctions screening with pre-release review (AML-02).

Supporting systems. Onboarding/KYC platform, transaction-monitoring engine, sanctions-screening tool, case management.

Evidence for audit. CDD files and approvals, alert logs and case files, screening configuration and logs, SAR register.

IT General Controls (ITGC)

Objective. Ensure the integrity, confidentiality and availability of systems supporting financial reporting and operations.

Key process steps

- Access provisioned on documented approval; least privilege applied (ITGC-01).
- Access recertified periodically; leavers removed promptly; privileged access logged (ITGC-01).
- Changes requested, tested, approved and released with dev/deploy segregation (ITGC-02).
- Backups monitored and restores tested; DR plan exercised (ITGC-03).

Key controls

- Approval-based provisioning and quarterly recertification (ITGC-01).

- Documented change lifecycle with segregation of duties (ITGC-02).
- Monitored backups, restore testing and annual DR exercise (ITGC-03).

Supporting systems. Identity & access management, change/ticketing system, backup & monitoring tools.

Evidence for audit. Access request and recertification records, privileged-access logs, change tickets with test and approval evidence, backup logs and DR test reports.

Information Security — ISO/IEC 27001 (SEC)

Objective. Protect information assets in line with the ISMS and Statement of Applicability.

Key process steps

- Information assets classified; risk assessed and treated (Cl.6, Cl.8).
- Controls selected per the Statement of Applicability; encryption and DLP applied (SEC-01).
- Security events logged, monitored and responded to.
- ISMS reviewed through internal audit and management review (Cl.9).

Key controls

- ISMS controls per SoA covering classification, encryption, DLP and monitoring (SEC-01).

Supporting systems. SIEM / security monitoring, encryption and DLP tooling, GRC platform.

Evidence for audit. Statement of Applicability, risk treatment plan, configuration evidence, monitoring alerts and incident records.

2.7 Audit Readiness Timeline (T-4 weeks to post-audit)

When	Activity	Owner
T–4 weeks	Confirm scope, objectives and timetable with auditors; brief Audit Committee	Head of Internal Control
T–3 weeks	Refresh RCM, narratives and policies; confirm control owners	CRO / Process Owners
T–2 weeks	Receive PBC list; assign owners; begin assembling evidence	Head of Internal Control
T–1 week	Complete evidence indexing; provision auditor read-only access; finalise logistics	Ops / CISO
Fieldwork	Manage requests through a single point of contact; log and resolve queries daily	Head of Internal Control
Post-audit	Agree findings; log deficiencies; track remediation to validated closure	Head of Internal Control

Part 3 · Enterprise Risk Management Framework

The ERM Framework establishes how the institution identifies, assesses, treats, monitors and reports risk across all categories, integrating COSO ERM (2017) principles with the ISO 31000 process and Nigerian supervisory expectations. ERM is positioned not as a compliance exercise but as a discipline that protects and creates value by aligning risk-taking with strategy and appetite.

COSO ERM Component	ISO 31000 Linkage	Application in the Institution
Governance & Culture	Leadership & commitment; integration	Board oversight, risk culture, Three Lines accountability
Strategy & Objective-Setting	Scope, context, criteria	Risk appetite linked to strategy and capital planning
Performance	Risk assessment & treatment	Risk register, ratings, KRIs and control responses
Review & Revision	Monitoring & review	Continuous monitoring, KRI tracking, assurance
Information & Reporting	Communication & consultation	Risk reporting to committees and the Board

3.1 Risk Assessment Methodology (5×5)

Score	Likelihood	Impact (highest dimension)
5	Almost certain — expected to occur	Severe — material to capital, licence or franchise
4	Likely — probably will occur	Major — significant financial / regulatory consequence
3	Possible — may occur	Moderate — contained but notable
2	Unlikely — not expected	Minor — limited, absorbed in normal operations
1	Rare — only in exceptional circumstances	Insignificant — negligible effect

Risk score = likelihood × impact, banded Low (1–3), Medium (4–6), High (8–12), Extreme (15–25). Inherent risk is rated before controls; residual risk after considering design and operating effectiveness. Impact is assessed across financial, regulatory, customer, operational and reputational dimensions, taking the highest applicable rating.

Part 4 · Risk Appetite Statement

Board Statement (qualitative). The institution pursues sustainable, risk-adjusted returns within a prudent and clearly defined risk appetite. It maintains capital and liquidity comfortably above regulatory minima, has no appetite for breaches of law, regulation or its code of conduct, no appetite for material financial-crime or data-protection failings, and a low appetite for operational disruption and reputational damage. It accepts measured credit, market and strategic risk where adequately controlled, priced and within approved limits.

Category	Appetite Statement	Tolerance (Amber)	Limit (Red)	Escalation
Financial	Stable, risk-adjusted earnings; capital above regulatory minima	CAR within 2% of minimum	CAR at regulatory minimum	CFO → Board Risk Cmte
Credit	Measured, well-secured credit growth within limits	NPL ratio 5%	NPL ratio 10%	CCO → Board Risk Cmte
Liquidity	Strong buffers; self-funded core book	LCR 110%	LCR 100%	Treasurer → ALCO → Board
Operational	Low appetite for disruption and process failure	Op loss 1% of revenue	Op loss 2% of revenue	COO → Op Risk Cmte
Compliance	Zero appetite for regulatory breaches	1 minor breach	Any material breach	CCO → Audit Cmte
Cybersecurity	Low appetite for security exposure	1 critical vuln past SLA	5 critical vulns past SLA	CISO → Board Risk Cmte
Reputational	Protect trust, brand and franchise	Adverse-event index 5	Adverse-event index 10	Comms → Board Chair

Part 5 · Key Risk Indicator (KRI) Framework

Key Risk Indicators provide forward-looking, quantitative signals of changing risk exposure, enabling intervention before a risk crystallises. The 52-indicator library spans ten domains — Financial Reporting, Treasury, Credit, Operations, Compliance, Cybersecurity, AML/KYC, Human Resources, Vendor Risk and Information Security — each with a definition, formula, threshold and automated RAG status. The full library is published as a standalone XLSX companion to this Toolkit.

KRI definition fields

- **Definition** — what the indicator measures and the risk it signals.
- **Formula** — the precise calculation and data source.
- **Thresholds** — Green (within appetite), Amber (tolerance approached), Red (limit breached).
- **RAG status** — derived automatically from the current value against thresholds.
- **Owner & frequency** — the accountable role and cadence of measurement.

Illustrative KRIs across the ten domains (extract — full library in companion XLSX)

#	Domain	Indicator	Green / Amber / Red	Owner
1	Financial Reporting	Manual journals above threshold not reviewed within 5 BD	0 / 1-3 / >3	Financial Controller
2	Financial Reporting	Late month-end close (BD past target)	0 / 1-2 / >2	Financial Controller
3	Treasury	LCR vs regulatory minimum	≥120% / 110-119% / <110%	Treasurer
4	Treasury	Open FX positions vs limit	≤75% / 76-90% / >90%	Treasurer
5	Credit	NPL ratio	≤3% / 3-5% / >5%	Chief Credit Officer
6	Credit	ECL coverage on Stage 3	≥60% / 50-59% / <50%	Chief Credit Officer
7	Operations	Operational losses vs revenue YTD	≤0.5% / 0.5-1% / >1%	COO
8	Operations	Reconciliation breaks open >30 days	≤5 / 6-15 / >15	Financial Controller
9	Compliance	Regulatory breaches in the quarter	0 / 1 / >1	CCO
10	Compliance	Overdue regulatory returns	0 / 1 / >1	CCO
11	Cybersecurity	Critical vulnerabilities past SLA	0 / 1 / >1	CISO
12	Cybersecurity	Privileged access not recertified	0 / 1-2 / >2	CISO
13	AML/KYC	Alerts open >30 days	0 / 1-5 / >5	MLRO
14	AML/KYC	CDD refresh overdue	0 / 1-10 / >10	MLRO
15	HR	Mandatory leave not taken in 12m	0 / 1-3 / >3	CHRO
16	HR	Outstanding starter/leaver actions	0 / 1-2 / >2	CHRO
17	Vendor Risk	Material vendors without current assurance report	0 / 1 / >1	COO
18	Vendor Risk	Tier-1 vendors with overdue review	0 / 1 / >1	COO
19	Information Security	Encryption non-conformities open	0 / 1-2 / >2	CISO
20	Information Security	DLP incidents past SLA	0 / 1-2 / >2	CISO

Part 6 · Internal Audit & Audit Committee Charters

6.1 Internal Audit Charter (extract)

Mission. To enhance and protect organisational value by providing independent, objective assurance and advisory services, applying a systematic, disciplined approach to evaluating and improving the effectiveness of governance, risk management and internal control.

Authority. The Audit Committee authorises Internal Audit to have full, free and unrestricted access to all functions, records, property, systems and personnel relevant to any engagement.

Independence. The Chief Audit Executive reports functionally to the Audit Committee and administratively to the Chief Executive. Internal Audit has no direct operational responsibility or authority over the activities it audits and does not design, install or operate controls.

Quality Assurance & Improvement Programme. Internal monitoring of every engagement, periodic internal self-assessment, and an external quality assessment at least once every five years by a qualified, independent assessor. Conformance with the IIA Global Internal Audit Standards is disclosed.

6.2 Audit Committee Charter (extract)

Area	Responsibilities
Financial reporting oversight	Review integrity of FS, significant judgements, accounting policies, going-concern; recommend FS to t
External audit oversight	Recommend appointment, remuneration and removal of external auditor; assess independence; reviev
Internal audit oversight	Approve internal audit charter, plan and budget; assess independence; review results and managemer
Risk & control oversight	Review effectiveness of internal control and, where delegated, the risk-management system; monitor r
Compliance & ethics	Oversee compliance with laws and regulations, the whistleblowing programme and the management o

Meetings. The Committee meets at least quarterly, and more often as required. A quorum is a majority of members, the majority of whom present are independent non-executives. The Committee holds private sessions with the external auditor and the Chief Audit Executive without management present.

Part 7 · Fraud Risk Management Framework

This framework sets out how the institution governs, prevents, detects, investigates and reports fraud, consistent with leading anti-fraud guidance and the institution's zero-tolerance stance. Fraud risk is assessed explicitly because conventional controls may not address the deliberate concealment and override that characterise fraud.

Control Theme	Preventive	Detective
Segregation & authority	Segregation of duties; delegated limits	Override and exception reporting
Access & system	Least-privilege access; dual control	Privileged-activity and audit-log review
Verification	Vendor and bank-detail call-backs	Three-way match and duplicate detection
People	Pre-employment screening; mandatory leave	Lifestyle / conflict-of-interest monitoring
Analytics	Preventive validation rules	Continuous data analytics and red-flag alerts

Illustrative Fraud Schemes & Key Controls

Scheme	Typical Red Flags	Key Controls
Payroll fraud	Ghost employees; unusual bank-detail changes; duplicate payments	HR-payroll reconciliation; bank-detail verification; starter/lea
Procurement fraud	Split orders; bid rigging; favoured suppliers	Competitive tendering; segregation; spend analytics; conflict d
Vendor fraud	Fictitious vendors; inflated or duplicate invoices	Vendor due diligence; dual master-data control; three-way mat
Financial-statement fraud	Period-end spikes; unusual manual journals; estimate manipulation	Journal review; reconciliations; analytical review; independent
Cyber fraud	Business email compromise; payment redirection; account takeover	Call-back verification; MFA; payment-change controls; transac

Whistleblowing. A confidential, independently operated channel allows staff and third parties to report concerns without fear of retaliation. Reports are logged, triaged by severity and escalated: routine matters to management, serious or senior-level matters directly to the Audit Committee Chair.

Part 8 · Regulatory Compliance Monitoring Framework

The framework provides a structured approach to identifying applicable regulatory obligations, monitoring compliance, managing regulatory change and testing the effectiveness of compliance controls. It is built around the Nigerian financial-services regulatory landscape.

Regulator	Focus	Illustrative Obligations
CBN	Banking prudential	Prudential ratios; statutory returns; AML/CFT/CPF regulations
SEC	Capital markets	Operator registration; periodic and event-driven returns
NGX	Listing & disclosure	Periodic financial disclosure; corporate actions; free-float
FRCN	Reporting & governance	IFRS compliance; NCCG 2018 apply-and-explain; annual returns
NDPC	Data protection	DPO appointment; compliance audit; annual filing under NDPA 2023
PenCom	Pensions	Timely pension remittance; compliance certificate
NFIU / SCUML	Financial crime	SAR/CTR filing; SCUML registration where applicable
NRS / State IRS	Tax	CIT, VAT, WHT, PAYE returns; transfer-pricing disclosures

Compliance Testing Methodology

Step	Activity
Scope	Select obligations and controls to test based on risk and regulatory priority.
Design test	Define attributes, population, sampling basis and evidence required.
Execute	Perform the test; document results and any exceptions.
Conclude	Rate effectiveness; root-cause exceptions; agree remediation and owner.
Report	Feed the compliance dashboard and Audit Committee; track to closure.

Part 9 · Audit Committee Dashboard Specification

Defines the seven indices presented to the Audit Committee, their calculation and RAG thresholds. Built in the companion XLSX (Audit Committee Dashboard Template 2026).

Indicator	Definition	Calculation	RAG bands
Audit Readiness Index	Progress against the audit-readiness checklist	Completed items ÷ total items	≥95% G · 85-94% A · <85% R
Control Effectiveness Index	Proportion of tested key controls operating effectively	Controls passed ÷ controls tested	≥95% G · 85-94% A · <85% R
Compliance Index	Regulatory obligations fully met	Obligations met ÷ total obligations	≥95% G · 85-94% A · <85% R
Risk Exposure Index	Weighted residual-risk profile (lower better)	(3×High + 2×Medium + 1×Low) ÷ (3×total)	≤45% G · 46-60% A · >60% R
Open Findings	Audit/compliance findings not yet closed	Count of open findings	≤5 G · 6-10 A · >10 R
Overdue Actions	Remediation actions past target date	Count past due date	0 G · 1-3 A · >3 R
High-Risk Issues	Open issues rated high/extreme	Count high/extreme open	0 G · 1-2 A · >2 R

Part 10 · 180-Day Implementation Roadmap

Phase	Objective	Key Activities
30 Days · Mobilise & Baseline	Stand up governance and baseline the program	Confirm the sponsor and steering committee; adopt ERM framework and appetite; ap
60 Days · Design & Embed	Embed frameworks into operations	Validate the Risk & Control Matrix; build the compliance monitoring plan; run the
90 Days · Test & Assure	Test controls and prove readiness	Execute first-cycle control testing; run compliance tests; complete control self-ass
180 Days · Optimise & Embed	Remediate, embed monitoring and deepen confidence	Remediate deficiencies; implement continuous KRI monitoring; refresh appetite vs s

Success measures. Audit Committee dashboard indices reach and sustain green status; high-risk findings are closed; an independent confirmation evidences conformance with COSO, ISO/IEC 27001, the IIA Global Internal Audit Standards and the Nigerian Code of Corporate Governance 2018.

About Outliers Professionals Ltd

Outliers Professionals Ltd is a Nigerian accounting, audit, governance, risk and intelligence firm serving boards, CFOs and CROs across financial services, manufacturing, public sector and SMEs. We design, implement and assure control environments, and we author the Outliers Professional Intelligence Platform — the regulatory, IFRS, tax, governance and risk reference library used by Nigerian filers. For a confidential briefing on adopting this Toolkit, visit outlierspro.com.