NCDF GROUP

NIGERIAN CAPITAL DEVELOPMENT FUND

Risk Management Framework

Institutional enterprise risk architecture for NCDF Holdings, regulated entities, Platform Companies, funds, SPVs, PPP projects, digital infrastructure and strategic partnerships.

Document Status	Board / Investor / Institutional Partner Review
Prepared For	NCDF Group - Nigerian Capital Development Fund
Version	Draft Framework v1.0
Date	June 2026

Confidential institutional document. This framework is intended for governance, risk oversight, investment-readiness, partner due diligence and enterprise control design. It is not a substitute for legal, regulatory, tax, actuarial, clinical, engineering or investment advice.

Contents

1. Executive Summary

NCDF Group requires a risk management framework that matches the ambition and complexity of its platform-company architecture. The Group is positioned across development investment management, capital markets, healthcare, HMO, housing, smart cities, agro-industrial infrastructure, fintech, agency banking, energy, education, cooperative commerce, diaspora investment and technology-enabled service delivery. This scale of activity creates significant upside, but it also requires a disciplined enterprise risk architecture that protects investors, regulators, communities, government partners, patients, beneficiaries and the NCDF brand.

This Risk Management Framework establishes the institutional standard for identifying, assessing, managing, monitoring, escalating and reporting risk across NCDF Group. It is designed to operate at five integrated levels: Group/HoldCo, regulated entities, Platform Companies, funds/investment vehicles, and project SPVs. The purpose is not to avoid risk; the purpose is to ensure that NCDF takes the right risks, at the right level, for the right return, with the right controls and within approved appetite.

5	4+	20+	12
Risk oversight layers	Core Platform Companies	Principal risk categories	Implementation workstreams

1.1 Institutional Risk Thesis

- NCDF Group is a development-investment platform; therefore, risk must be governed as an enterprise value protection system, not as a compliance afterthought.
- The Group should operate a consolidated risk view while preserving regulatory ring-fencing for licensed and regulated businesses.
- Each Platform Company must maintain its own risk register, key risk indicators and management accountability, but Group must consolidate risk exposure and strategic contagion risk.
- Capital raising, fund management, securities activities, healthcare delivery, HMO operations, fintech, PPP projects and construction must each be controlled under sector-specific standards.
- Investor confidence will be materially strengthened where NCDF can demonstrate risk appetite, independent oversight, documented authority, controlled related-party transactions, reliable reporting and a functioning escalation protocol.

1.2 Framework Outcomes

Outcome	Institutional Meaning for NCDF Group
Capital protection	Capital is deployed only into approved platforms, projects and instruments that have passed documented risk, legal, regulatory, commercial, ESG and financial due diligence.
Regulatory confidence	Regulators can see clear governance separation, compliance ownership, auditable policies, board oversight and breach escalation.
Investor readiness	Investors receive a structured view of portfolio risk, platform risk, use-of-proceeds risk, valuation risk, liquidity risk, governance risk and reporting controls.
Operational resilience	Critical activities can continue through incidents, technology disruption, project delays, partner failure, market volatility or regulatory changes.
Reputation protection	The NCDF brand is protected through conduct standards, complaints controls, stakeholder management, patient/service-user safeguarding and public communications discipline.
Impact integrity	Development outcomes are measured, verified and protected from greenwashing, impact exaggeration, weak beneficiary controls or poor social safeguards.

Board adoption recommendation

The Board should adopt this framework as the Group ERM standard and mandate each Platform Company, regulated entity, fund and SPV to produce a risk register and control implementation plan within 60 days of adoption.

2. Purpose, Scope and Institutional Context

Purpose. This framework defines how NCDF Group should govern enterprise risk across its investment, operating, regulated, project and digital ecosystem. It provides the operating architecture for risk accountability, risk appetite, risk taxonomy, assessment methodology, reporting, escalation, risk registers, control ownership and board oversight.

2.1 Scope of Application

Layer	Included Entities / Activities	Risk Governance Requirement
Group / Sponsor Layer	NCDF Holdings Limited, Group strategy, capital allocation, brand, group policies, governance standards and strategic partnerships.	Board-approved ERM framework, Group risk appetite, consolidated risk register, central policy architecture and Group-level reporting.
Regulated Capital-Market Layer	NCDF Investment Management Plc, NCDF Securities Limited, fund management, issuing-house activities, securities transactions, investor onboarding and capital raising.	Regulatory compliance, investment committee controls, AML/CFT, suitability, conflicts management, fund governance, disclosure controls and market-conduct oversight.
Platform Company Layer	Fatherland Smart Cities, LifeCome Healthcare & Health Energy, AfriGo Digital Economic Zone, Konto Financial Group and other platform companies.	Platform-specific risk register, board/management risk ownership, operational risk controls, financial controls and quarterly risk certification.
Fund / Vehicle Layer	NCDF Opportunity Growth Fund, NCDF Diaspora Impact Fund, Real Estate Equity Fund, Green Infrastructure Bond programme and future vehicles.	Offering-document risk alignment, fund risk register, investment restrictions, valuation controls, liquidity controls, investor reporting and trustee/custodian oversight where applicable.
Project / SPV Layer	Affordable housing estates, healthcare concessions, agro-industrial parks, green infrastructure, transport, technology assets and state-based PPP projects.	Project gate controls, SPV governance, feasibility validation, procurement controls, construction monitoring, contract management and environmental/social safeguards.
Digital and Data Layer	AfriGoOS, CoopX / NCDFCOOP, LifeCome AleraAI, Konto digital channels, member dashboards, data infrastructure and AI-enabled services.	Cybersecurity, data protection, privacy-by-design, change management, platform resilience, user onboarding controls and AI governance.

Framework principle

Risk management must follow the economic substance of the activity. A risk does not disappear because it is housed in a subsidiary or SPV. Group must maintain visibility, while each entity retains primary accountability for the risks it originates and manages.

3. Risk Philosophy and Governance Principles

NCDF Group's risk philosophy is to take informed, measured and strategically justified risk in sectors where the Group has a development mandate, institutional capability, partner alignment and credible value-creation pathway. The Group should not pursue opportunities merely because they are large, politically attractive or commercially fashionable. Every opportunity must be evaluated against capital protection, regulatory compliance, execution capacity, governance substance, stakeholder value and impact integrity.

3.1 Core Principles

Principle	NCDF Application
Risk is owned by the business	Each Platform Company, fund, project and operating team owns the risks created by its decisions. The Group Risk function provides oversight, challenge and consolidation.
Board oversight is non-delegable	Boards and board committees must retain accountability for risk appetite, material exposures, major transactions, related-party transactions, capital allocation and regulatory breaches.

Principle	NCDF Application
No capital without controls	Capital should not be raised, accepted, committed or deployed without verified use-of-proceeds controls, sign-off authority, legal documentation, bank/account controls and reporting obligations.
Ring-fencing protects value	Regulated entities, funds, SPVs and platforms must maintain legal, accounting, governance and cash-flow separation to avoid contagion, regulatory breach or investor confusion.
Risk-adjusted return matters	Projects should be assessed not only by headline revenue or impact potential, but by execution risk, funding risk, counterparty risk, liquidity risk, regulatory risk and reputational risk.
Transparency builds confidence	Investors, boards, regulators and partners require accurate reporting of material risks, breaches, delays, assumptions, conflicts and remediation actions.
Impact must be verifiable	Impact claims must be supported by measurable indicators, beneficiary records, transparent methodology and independent review where appropriate.

4. NCDF Group Enterprise Risk Architecture

The risk architecture should be designed as a layered operating system. Group defines standards, regulated entities comply with sector rules, Platform Companies execute business activity, funds hold investor capital under specific mandates, and SPVs deliver ring-fenced projects. Risk information must move upward to the Board and downward into management action.

Risk Layer	Primary Accountability	Core Controls	Escalation Destination
Group / Sponsor	NCDF Holdings Board, Group CEO/Chairman, Group Risk Committee	Group risk appetite, policy architecture, consolidated risk dashboard, delegation of authority, related-party governance	Group Board / Board Risk Committee
Regulated Entities	Entity Board, MD/CEO, Compliance Officer, Risk Officer	Regulatory compliance plan, AML/CFT, investor onboarding, disclosure controls, fund/securities policies	Entity Board / Regulator / Group Board
Platform Companies	Platform Board, Managing Director, Platform Risk Owner	Operating risk register, budget controls, HR controls, procurement rules, partner due diligence, monthly risk reports	Platform Board / Group Risk
Funds / Investment Vehicles	Fund Manager, Investment Committee, Trustee/Custodian where applicable	Mandate limits, investment restrictions, valuation policy, liquidity monitoring, investor reporting	Investment Committee / Fund Board / Trustee
Project SPVs	SPV Board, Project Director, EPC/O&M teams	Project gates, contracts, milestone monitoring, budget and schedule controls, ESG safeguards, insurance	SPV Board / Platform Board / Group Risk

4.1 Three Lines of Defence Model

Line	NCDF Group Role	Examples of Activities
First Line - Business and Operations	Platform Companies, regulated entities, funds, SPVs, project teams and functional managers own and manage risks in day-to-day activities.	Risk identification, control operation, budget control, compliance with policies, incident reporting, contract management, due diligence execution.
Second Line - Risk, Compliance and Control Functions	Group Risk, Compliance, Legal, Finance, Internal Control, Data Protection, ESG and Clinical Governance functions set standards and challenge management.	Risk framework, policy review, compliance monitoring, AML/CFT oversight, risk dashboard, regulatory horizon scanning, training, control testing.
Third Line - Internal Audit / Independent Assurance	Internal audit or outsourced assurance independently reviews whether governance, controls and risk management are operating effectively.	Risk-based audits, fund-control reviews, IT security assurance, procurement audits, project gate reviews, regulatory compliance audits, corrective-action tracking.

5. Board, Committee and Management Risk Governance

Risk governance must be formal, documented and evidenced. NCDF Group should operate a clear hierarchy of authority, reporting and challenge. This protects the Group against informal decision-making, unapproved commitments, mandate drift, concentration exposure, uncontrolled related-party transactions and weak investor communication.

5.1 Governance Bodies and Responsibilities

Governance Body	Core Risk Responsibilities	Minimum Outputs
Group Board	Approve risk appetite, ERM framework, major capital commitments, new platforms, material transactions, regulated entity oversight and risk escalation thresholds.	Annual risk appetite statement; quarterly risk dashboard review; approval minutes; risk policy approval.
Board Risk & Compliance Committee	Oversee risk register, compliance universe, regulatory breaches, risk appetite breaches, incident reports, risk remediation and assurance outcomes.	Quarterly risk committee pack; breach log; remediation tracker; regulatory update summary.
Investment Committee	Approve investments, funds, transactions and project commitments within mandate, after risk-adjusted review and conflict checks.	Investment memos; risk scorecards; IC minutes; decision conditions; post-investment monitoring notes.
Audit & Finance Committee	Oversee financial reporting, audit, treasury risk, internal controls, related-party transactions, budgets, valuations and financial disclosures.	Internal control reports; audit plan; related-party register; valuation review; cash control certification.
Platform Company Boards	Oversee platform-specific risk appetite, operational risk, strategy execution, major contracts, subsidiaries, SPVs and platform risk register.	Platform risk dashboard; monthly management accounts; operational risk register; board action log.
Management Risk Forum	Coordinate cross-functional risk review across legal, finance, compliance, operations, technology, HR, ESG and business development.	Monthly risk meeting minutes; emerging risk list; incident log; control improvement plan.
Internal Audit / Independent Assurance	Provide independent review of control effectiveness and governance discipline.	Annual audit plan; audit reports; corrective action follow-up; board assurance memo.

Non-negotiable governance control

Any material investment, fund launch, securities issuance, PPP commitment, new SPV, related-party transaction, external guarantee, debt facility, acquisition, concession or regulatory filing must have documented approval at the appropriate authority level before commitment.

6. Risk Appetite Framework

Risk appetite defines the type and level of risk NCDF Group is willing to accept in pursuit of strategy. Risk appetite should be approved by the Group Board, cascaded to Platform Companies and translated into measurable thresholds, mandates, authorities, investment limits, project gates and breach escalation requirements.

6.1 Group-Level Risk Appetite Statement

Proposed risk appetite statement

NCDF Group will accept disciplined, transparent and risk-adjusted exposure to development sectors where the Group has governance capability, regulatory clarity, credible partners, executable projects, adequate capital controls and measurable impact. The Group has low appetite for regulatory breach, investor misrepresentation, uncontrolled related-party transactions, weak safeguarding, unmanaged cyber/data risk, undisclosed conflicts, unapproved commitments, poor clinical governance, unsafe construction, AML/CFT weakness or reputational conduct failure.

6.2 Risk Appetite by Category

Risk Category	Risk Appetite	Practical Interpretation
Strategic growth risk	Moderate	NCDF may enter ambitious sectors but only where there is a documented business case, capability plan, capital plan and governance structure.
Regulatory and compliance risk	Low	No tolerance for deliberate non-compliance; all regulated activity must be licensed, supervised or executed through appropriately authorised structures.
Capital raising and investor disclosure risk	Low	Investor materials must be accurate, approved, consistent with offering documents and free from misleading return claims.
Investment and portfolio risk	Moderate	Risk is acceptable where it is consistent with approved mandate, due diligence, concentration limits and exit strategy.
Liquidity and solvency risk	Low to moderate	The Group should avoid unfunded commitments and ensure cash-flow visibility before project or fund obligations are accepted.
Project execution and construction risk	Moderate	Acceptable only with feasibility, budget, contract, insurance, milestone, procurement and engineering controls.
Healthcare and clinical risk	Low	Patient safety, clinical governance and provider quality controls must override revenue considerations.
HMO claims and actuarial risk	Low to moderate	Products must be priced with service limits, authorisation rules, claims controls, provider tariffs and reserve discipline.
Technology, cyber and data risk	Low	Digital platforms must apply security-by-design, privacy-by-design, access controls and incident response.
Reputation and stakeholder risk	Low	No appetite for avoidable reputational harm from weak communication, service failure, unethical conduct or exaggerated impact claims.
ESG, safeguarding and community risk	Low	Projects must avoid unmanaged harm to communities, environment, vulnerable people, patients, children, employees and beneficiaries.

7. Group Risk Taxonomy

A common taxonomy enables consistent risk identification, scoring, ownership and reporting across the Group. Each Platform Company and SPV should map its risk register to this taxonomy while adding sector-specific risks as required.

Risk Category	Examples of Exposure	Primary Owners
Strategic Risk	Wrong sector choices, weak business model, overexpansion, loss of focus, mandate drift, poor integration of platforms.	Group Board; Strategy Office; Platform Boards
Governance Risk	Weak board oversight, undocumented authority, related-party ambiguity, conflicts of interest, insufficient independence, poor minutes.	Company Secretary; Legal; Board Committees
Regulatory / Compliance Risk	Licensing breach, late filings, non-compliant capital raise, fund-rule breach, HMO guideline breach, CBN/SEC/NHIA exposure.	Compliance Officer; Legal; Regulated Entity Boards
Capital Formation Risk	Unclear offering terms, unsuitable investors, disclosure gaps, use-of-proceeds mismatch, failure to close capital stack.	Investment Committee; Corporate Finance; Legal
Investment / Portfolio Risk	Due diligence weakness, valuation error, concentration, illiquidity, failed exits, investee underperformance.	Fund Manager; Investment Committee
Credit / Counterparty Risk	Partner default, buyer non-payment, government receivable delay, provider overbilling, borrower default.	Finance; Risk; Commercial Teams
Liquidity / Treasury Risk	Cash mismatch, FX exposure, unfunded commitments, weak account controls, poor cash forecasting.	CFO; Treasury; Audit & Finance Committee
Project / PPP Risk	Feasibility error, land title issues, concession risk, permitting delays,	Project Director; SPV Board;

Risk Category	Examples of Exposure	Primary Owners
	construction cost overrun, political changes.	Platform Board
Operational Risk	Process failure, poor staffing, weak SOPs, procurement leakage, vendor failure, inadequate training.	COO; Platform Operations; Internal Control
Clinical / HMO Risk	Patient safety incidents, provider network weakness, claims leakage, tariff disputes, authorisation failure, fraud/waste/abuse.	Chief Medical Officer; HMO MD; Clinical Governance
Technology / Cyber Risk	System downtime, data breach, cyberattack, API weakness, unauthorised access, payment platform disruption.	CTO; CISO/Data Protection Officer
Data / AI Risk	Poor data governance, personal data misuse, biased AI decisions, inadequate consent, weak model governance.	DPO; CTO; AI Governance Lead
Legal / Contract Risk	Unclear rights, unenforceable agreements, litigation, indemnity exposure, weak dispute resolution.	Legal Counsel; Contract Owners
Financial Crime Risk	AML/CFT weakness, sanctions breach, fraud, bribery, corruption, politically exposed person risk.	Compliance; AML Officer; Internal Audit
ESG / Impact Risk	Environmental harm, social opposition, poor safeguards, greenwashing, impact exaggeration, weak grievance mechanism.	ESG Lead; Project Teams; Board Risk Committee
Reputational Risk	Public controversy, investor complaints, stakeholder conflict, poor service delivery, media escalation.	Communications; CEO; Board Risk Committee
People / Culture Risk	Key-person dependency, weak recruitment, misconduct, inadequate training, poor performance management.	HR; Executive Management
Macroeconomic / Country Risk	Inflation, FX volatility, interest rates, policy change, fiscal constraints, political instability.	Strategy; Treasury; Board

8. Risk Management Process and Methodology

The NCDF risk process should follow a disciplined cycle: identify, assess, respond, control, monitor, report and learn. The methodology is intentionally simple enough for consistent use across Platform Companies, but robust enough for board reporting, investor due diligence and regulatory assurance.

8.1 Risk Assessment Cycle

Stage	Application
1. Identify	Capture risks from strategy, capital raising, operations, projects, compliance, contracts, technology, people, ESG and external environment.
2. Assess	Score inherent likelihood and impact; evaluate velocity, control strength and residual risk.
3. Respond	Avoid, reduce, transfer, accept or exploit the risk, with documented rationale and approval.
4. Control	Design controls, assign owners, set deadlines and document evidence requirements.
5. Monitor	Track KRIs, breaches, incidents, audit findings, delays, cost movements and emerging risks.
6. Report	Escalate material risks to management forums, Platform Boards, Group Risk Committee and Group Board.
7. Learn	Use incidents, audits, regulatory feedback and project post-mortems to update controls and policies.

8.2 Risk Scoring Matrix

Score	Likelihood	Impact	Risk Response

Score	Likelihood	Impact	Risk Response
1	Rare	Insignificant: manageable within routine operations.	Monitor through normal management controls.
2	Unlikely	Minor: limited financial, operational or stakeholder effect.	Manage locally; report if trend increases.
3	Possible	Moderate: could affect timelines, costs, compliance or service quality.	Action plan required; platform-level reporting.
4	Likely	Major: material financial, regulatory, clinical, project, investor or reputational effect.	Immediate senior management attention; Board Risk Committee notification.
5	Almost Certain	Severe: threatens licence, capital raise, patient safety, fund integrity, solvency, major project or brand trust.	Immediate escalation to Group Board/appropriate regulator where required; crisis response.

Impact / Likelihood	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Risk heat map: residual risk score = likelihood x impact. Scores 1-5 are low, 6-10 moderate, 11-15 high and 16-25 critical.

9. Platform Company Risk Profiles

Each Platform Company has a distinct risk profile. The Group framework must therefore be applied through platform-specific controls, risk owners and reporting dashboards.

9.1 Fatherland Smart Cities Platform Company

Core exposure	Affordable housing, smart city development, estate infrastructure, land, construction, diaspora homebuyer products, real estate equity structures and state partnerships.
Principal risks	Land/title risk; construction cost overrun; sales/offtake risk; homebuyer trust risk; contractor performance; infrastructure delivery; regulatory approvals; community relations; FX/import cost exposure; completion risk.
Priority controls	Land due diligence; SPV ring-fencing; EPC contract controls; quantity surveying; milestone-based disbursement; independent project monitoring; escrow/use-of-proceeds controls; customer disclosure; grievance channels; insurance.
Board focus	Project pipeline approval, land bank quality, sales commitments, financing plan, contractor capacity, construction dashboard, handover risk and homebuyer protection.

9.2 LifeCome Healthcare & Health Energy Platform Company

Core exposure	Hospitals, concessions, HMO, provider networks, clinical operations, health energy, AleraAI, digital continuity of care and healthcare partnerships.
Principal risks	Patient safety; clinical governance failure; NHIA/HMO compliance; claims leakage; provider quality; drug/service limits; complaints; data privacy; AI clinical decision risk; staffing; medical liability; emergency response.
Priority controls	Clinical governance board; medical audit; provider credentialing; tariff schedule; authorisation rules; claims review; incident reporting; safeguarding; data protection impact assessments; technology validation; professional indemnity insurance.
Board focus	Patient safety, regulator readiness, HMO reserve discipline, provider quality, claims ratios, clinical KPIs, complaint trends, technology safety and operational readiness.

9.3 AfriGo Digital Economic Zone Platform Company

Core exposure	Agro-processing parks, export processing and packaging, digital trade infrastructure, cooperative producer aggregation, logistics, quality assurance and buyer access.
Principal risks	Commodity price volatility; producer quality inconsistency; export documentation; food safety; logistics disruption; buyer default; working capital mismatch; warehouse controls; equipment downtime; community/stakeholder risk.
Priority controls	Quality standards; supplier onboarding; warehouse inventory controls; buyer due diligence; export documentation checklists; insurance; working capital policies; traceability; ESG safeguards; equipment maintenance.

Board focus	Pipeline of producers/buyers, quality certification, export compliance, inventory risk, working capital cycle, offtake contracts, logistics partners and food safety.

9.4 Konto Financial Group Platform Company

Core exposure	Fintech, agency banking, microinsurance, finance house/development finance, payments, agents, customer onboarding and financial inclusion services.
Principal risks	Regulatory licensing; AML/CFT; agent fraud; operational resilience; cybersecurity; customer funds protection; product suitability; consumer complaints; liquidity; credit risk; partner-bank dependency; claims/insurance risk.
Priority controls	Regulatory licensing roadmap; AML/KYC; agent onboarding and monitoring; transaction limits; reconciliation controls; customer protection; cybersecurity; fraud analytics; complaints procedure; partner-bank SLAs; business continuity.
Board focus	Licensing milestones, capital adequacy, transaction monitoring, agent network quality, reconciliation breaks, fraud loss, customer complaints, cybersecurity readiness and liquidity.

10. Capital Formation, Fund and Investor Risk Controls

Capital formation is central to NCDF Group's strategy. The Group must therefore operate disciplined controls around investor communications, suitability, offering documentation, use of proceeds, fund mandates, valuations, reporting and conflicts.

Control Area	Required Institutional Control	Evidence / Output
Investor materials	All teasers, pitch decks, PPMs, IMs, term sheets and digital marketing materials must be reviewed by Legal, Compliance and the approving business owner before circulation.	Approved document log; version control; approval memo.
Investor suitability	Investor onboarding must confirm whether the investor is institutional, qualified, sophisticated, retail, diaspora, cooperative member or otherwise subject to restrictions.	KYC pack; suitability form; risk acknowledgement.
Use of proceeds	Use-of-proceeds budgets must map to approved capital plan, escrow/account controls and reporting obligations.	Use-of-proceeds register; bank mandate; disbursement approval trail.
Disclosure risk	Financial forecasts, valuation claims, impact claims and return expectations must be evidenced and caveated appropriately.	Disclosure checklist; assumptions appendix; risk factors.
Fund mandates	Each fund must have investment restrictions, eligible assets, concentration limits, leverage limits, valuation policy and liquidity policy.	Fund manual; investment policy statement; IC checklist.
Conflicts and related parties	Any transaction involving Group entities, directors, sponsors or related parties must be disclosed, reviewed and approved under the related-party policy.	Related-party register; conflict declarations; board approval.
Investor reporting	Investors must receive timely, accurate and consistent reports according to contractual and regulatory obligations.	Quarterly investor report; fund NAV report; project dashboard.

Investor protection standard

NCDF should treat disclosure quality, risk-factor transparency, use-of-proceeds control and investor reporting as core value-creation tools. These controls reduce fundraising friction and support institutional due diligence.

11. Project, PPP and SPV Risk Controls

NCDF's project pipeline should be governed through stage-gate discipline. No project should move from concept to capital deployment without passing defined feasibility, legal, financial, technical, ESG, partner, contract and governance gates.

Project Gate	Minimum Risk Requirements	Decision Output
Gate 0 - Strategic fit	Confirm alignment with NCDF mandate, platform strategy, impact thesis and investor appetite.	Strategic screening note.
Gate 1 - Concept	Define problem, project scope, sponsor, location, beneficiaries, commercial logic and preliminary risk profile.	Concept note and initial risk screen.
Gate 2 - Feasibility	Technical, legal, market, financial, ESG, land/title, regulatory and stakeholder feasibility.	Feasibility pack and risk register.
Gate 3 - Structuring	SPV structure, contractual framework, funding plan, risk allocation, tax/accounting review and governance documents.	Structuring memo and approval conditions.
Gate 4 - Investment approval	Investment memo, financial model, due diligence, risk scorecard, ESG plan, legal opinions and capital approvals.	Investment Committee / Board approval.
Gate 5 - Execution	Procurement, contracting, insurance, project management office, milestone	Execution mandate

Project Gate	Minimum Risk Requirements	Decision Output
	disbursement and monitoring dashboard.	and control tracker.
Gate 6 - Operations	O&M plan, revenue collection, compliance, service delivery, asset management, insurance and reporting.	Operational risk dashboard.
Gate 7 - Exit / Refinancing	Valuation, refinancing, sale, listing, investor exit, asset transfer or concession handback plan.	Exit or refinancing memo.

12. Financial, Treasury and Balance Sheet Risk Controls

Financial discipline must be central to the Group risk framework because NCDF will manage sponsor capital, investor funds, project cash flows, platform operating budgets, regulated entity capital and SPV financing commitments.

Risk Area	Control Standard
Cash and bank controls	Bank mandates must require dual signatory or tiered approval. Fund accounts, SPV accounts, operating accounts and client/investor monies must be separated where required.
Budgetary control	Annual budgets must be approved by the relevant board. Budget variance above approved threshold must be explained and remediated.
Liquidity forecasting	Rolling 13-week cash-flow forecasts should be maintained for material platforms, funds and SPVs.
FX risk	Foreign currency commitments must be mapped to natural hedges, revenue currency, import exposure and board-approved hedging approach where appropriate.
Debt and leverage	Debt facilities, guarantees and contingent liabilities must be approved under the delegation of authority and covenant monitoring system.
Valuation risk	Investments, assets, fund units and project interests must be valued using documented methodology, independent review where needed and consistency with investor materials.
Financial reporting	Monthly management accounts, quarterly board reports and annual audited financial statements must be prepared on time and reconciled to budgets and project dashboards.

13. Regulatory, Compliance, AML/CFT and Conduct Risk

NCDF Group operates across sectors that may be supervised by different regulators or affected by different laws and guidelines. A central compliance universe should be maintained and updated periodically, while each regulated entity remains responsible for its own obligations.

Regulatory Area	Relevant NCDF Exposure	Required Control
Capital markets / securities	Private placements, funds, securities issuance, fund management, issuing-house activities and investor communication.	SEC compliance calendar, approved offering documents, investor suitability, risk factors, custody/trustee controls and reporting.
Healthcare / HMO	LifeCome HMO, hospitals, provider networks, claims, tariffs, member services and NHIA interactions.	NHIA guideline compliance, provider contracts, claims SOP, authorisation rules, complaints procedure and clinical governance.
Financial services / payments	Konto fintech, agency banking, payments, finance house, microinsurance and partner-bank arrangements.	CBN/NAICOM/NIBSS/partner-bank compliance map as applicable, KYC/AML, transaction monitoring, agent controls and consumer protection.
Data protection	Patient data, investor data, member data, AI training data, digital platforms, employee data and cross-border processing.	Data inventory, lawful basis, DPIA, consent where required, DPO, privacy notices, access controls and breach response.
PPP / infrastructure	Concessions, government partnerships, state projects, healthcare infrastructure, agro-industrial parks and smart city projects.	OBC/FBC discipline, concession agreement review, procurement integrity, contract risk allocation and stakeholder engagement.
Corporate governance	Group, platform, regulated entity and SPV boards.	Board charters, committee terms, conflict declarations, minutes, annual board evaluation and apply-and-explain governance reporting where applicable.
AML/CFT / sanctions / anti-bribery	Capital raising, fintech, agency network, government contracts, donor funds, diaspora capital and procurement.	KYC, PEP screening, sanctions checks, suspicious activity reporting, gifts register, whistleblowing and anti-bribery training.

Compliance universe requirement

The Group should maintain one central compliance universe, but each entity must maintain its own regulatory obligation tracker. This prevents Group-level visibility gaps while preserving entity-level accountability.

14. Technology, Cybersecurity, Data Protection and AI Risk

NCDF's technology layer is a strategic asset and a material risk area. AfriGoOS, CoopX / NCDFCOOP, LifeCome AleraAI, Konto digital channels and member dashboards will handle sensitive data, transactions, investor/member onboarding, clinical workflows, cooperative records and operational reporting. These platforms require security-by-design and privacy-by-design.

Control Domain	Required Controls
Cyber governance	Board-approved cyber risk policy, named technology/cyber owner, critical asset inventory and cyber risk reporting.
Access management	Role-based access, multi-factor authentication for privileged users, periodic access review and leaver access removal.
Data protection	Data mapping, lawful basis, retention schedule, data sharing agreements, DPIAs and breach notification protocol.
Secure development	Code review, testing, vulnerability scanning, change approval, release management and third-party software review.

Control Domain	Required Controls
Platform resilience	Backups, disaster recovery, uptime targets, incident response, recovery time objectives and system monitoring.
Third-party technology risk	Vendor due diligence, SLA, data processing agreements, security questionnaires and exit arrangements.
AI governance	Model purpose definition, human oversight, bias testing, clinical/data validation, audit trail, explainability and restriction on unauthorised clinical decision automation.
Fraud monitoring	Transaction monitoring, anomaly alerts, agent monitoring, member/investor onboarding checks and exception reporting.

15. ESG, Safeguarding and Impact Risk

NCDF's development mandate creates a strong impact proposition, but it also creates heightened responsibility to ensure environmental and social safeguards, beneficiary protection, community engagement and truthful impact reporting.

Risk Area	Minimum Control Standard
Environmental risk	Environmental screening, mitigation plans, permits, waste management, energy-use standards and monitoring for construction, healthcare, agro-processing and energy projects.
Social and community risk	Stakeholder mapping, community engagement, grievance mechanism, local employment plan and conflict-sensitive project planning.
Safeguarding	Protection controls for patients, vulnerable service users, children, beneficiaries, employees and community participants.
Labour and human rights	Fair recruitment, safe working conditions, contractor labour standards and whistleblowing channels.
Impact integrity	Impact metrics must be defined before project launch, measured periodically and separated from marketing claims.
Greenwashing / impact exaggeration	No ESG or impact claim should be made without evidence, methodology and reporting ownership.
Health and safety	Construction safety, hospital safety, emergency response, infection control and occupational health requirements must be embedded in project and operational SOPs.

16. Risk Reporting, KRIs and Escalation Protocol

Risk information must be converted into decision-ready reporting. The goal is not to produce lengthy registers that no one uses; the goal is to deliver accurate, timely and actionable insight to the correct decision-makers.

Report	Prepared By	Frequency	Recipients
Platform Risk Dashboard	Platform Risk Owner / MD	Monthly	Platform Board, Group Risk
Group Consolidated Risk Dashboard	Group Risk / Compliance	Quarterly	Board Risk & Compliance Committee, Group Board
Investment / Fund Risk Report	Fund Manager / Investment Team	Quarterly or as mandated	Investment Committee, Fund Board, Investors where required
Project Risk Report	Project Director / PMO	Monthly during execution	SPV Board, Platform Board, Group Risk

Report	Prepared By	Frequency	Recipients
Regulatory Compliance Report	Compliance Officer	Monthly / Quarterly	Entity Board, Group Compliance, Board Risk Committee
Incident and Breach Report	Incident Owner	Immediate / within 24-72 hours depending on severity	CEO, Risk, Legal, Board Chair, regulator where required
Internal Audit Report	Internal Audit / Independent Assurance	As per annual audit plan	Audit Committee, Board Risk Committee

16.1 Example Key Risk Indicators

KRI Area	Example Indicators
Capital raising	Investor conversion rate, unresolved investor queries, disclosure exceptions, KYC delays, use-of-proceeds variances.
Funds / investments	Portfolio concentration, overdue reporting, valuation exceptions, covenant breaches, investment committee conditions outstanding.
Projects	Budget variance, schedule slippage, unresolved permits, contractor claims, safety incidents, milestone failures.
Healthcare / HMO	Claims ratio, claims turnaround, provider disputes, member complaints, adverse clinical incidents, authorisation exceptions.
Fintech / agency	Failed reconciliations, fraud loss, dormant agents, chargebacks, customer complaints, system downtime.
Cyber / data	Critical vulnerabilities, overdue patches, access review exceptions, data incidents, failed backups, phishing results.
Compliance	Regulatory filings late, policy breaches, training completion, AML alerts, unresolved audit findings.

17. Crisis, Incident and Business Continuity Management

NCDF Group should maintain a documented incident management and business continuity framework for events that may threaten operations, capital, patient safety, investor trust, regulatory standing, project delivery or technology resilience.

Severity	Examples	Escalation Requirement
Level 1 - Low	Minor operational issue, local complaint, small process error with no material impact.	Managed by local owner; recorded in incident log.
Level 2 - Moderate	Service disruption, complaint escalation, minor regulatory concern, budget variance, small data incident.	Platform MD and Group Risk informed within 48 hours; remediation plan required.
Level 3 - High	Material project delay, serious complaint, fraud suspicion, clinical incident, cyber incident, investor disclosure issue.	CEO, Legal, Compliance and Board Risk Chair informed within 24 hours; formal incident response.
Level 4 - Critical	Licence threat, major data breach, patient death/serious harm, fund/investor capital issue, major fraud, public crisis.	Immediate escalation to Group Board and external advisers; regulator/stakeholder notification where required; crisis committee activated.

Business continuity priority

Critical services should have continuity plans: investor communication, fund accounting, HMO claims, hospital

operations, payment systems, digital platforms, construction sites, customer service, finance and regulatory reporting.

18. Implementation Roadmap

The framework should be implemented through a disciplined programme that translates policy into behaviour, reporting and evidence.

Phase	Timing	Priority Actions	Outputs
Phase 1 - Foundation	0-30 days	Board adoption; appoint Group Risk Owner; approve risk appetite; create risk policy inventory; identify risk owners across entities.	Approved framework; implementation memo; risk owner map; initial risk calendar.
Phase 2 - Entity risk registers	31-60 days	Prepare risk registers for Group, regulated entities, Platform Companies, funds and priority SPVs; map compliance universe.	Entity risk registers; compliance trackers; top 20 Group risks.
Phase 3 - Control design	61-100 days	Implement delegation matrix, investment checklist, related-party register, incident log, KRI dashboards and reporting templates.	Risk dashboard pack; control templates; escalation protocol.
Phase 4 - Assurance readiness	3-6 months	Conduct control self-assessment; launch training; perform internal audit readiness review; close high-priority gaps.	Control self-assessment; training records; audit readiness report.
Phase 5 - Institutional maturity	6-12 months	Embed board reporting, platform dashboards, fund reporting, project gates, cyber/data reviews and ESG safeguards.	Quarterly board risk reports; ESG risk reports; annual risk assurance plan.
Phase 6 - Continuous improvement	12-24 months	Independent assurance, policy refresh, automation of dashboards, stress testing and investor-grade risk reporting.	Annual ERM report; independent assurance findings; improved risk maturity score.

19. Appendices: Templates and Reference Anchors

Appendix A - Standard Risk Register Template

Field	Description
Risk ID	Unique reference number.
Risk Category	Mapped to NCDF Group taxonomy.
Risk Description	Clear description of event, cause and consequence.
Entity / Platform / SPV	Where the risk is owned.
Inherent Likelihood	Score 1-5 before controls.
Inherent Impact	Score 1-5 before controls.
Existing Controls	Controls currently in place.
Control Effectiveness	Strong, adequate, weak or absent.
Residual Likelihood	Score 1-5 after controls.
Residual Impact	Score 1-5 after controls.
Risk Rating	Residual likelihood x residual impact.
Risk Owner	Named accountable person.
Treatment Plan	Actions to reduce, transfer, avoid, accept or exploit.
Target Date	Date by which action must be completed.
Status	Open, in progress, overdue, closed.
Escalation Required	Yes/no and escalation destination.

Appendix B - Top Enterprise Risks for Immediate Board Visibility

Priority Risk	Reason for Board Attention	Immediate Mitigation
Regulatory authorisation and compliance sequencing	NCDF platforms include capital markets, HMO/healthcare, fintech, agency banking, microinsurance, funds and PPP structures with different approval requirements.	Maintain regulatory roadmap, appoint compliance owners, avoid premature regulated activity and obtain legal opinions before launch.
Capital raise disclosure and investor suitability	Multiple investment routes increase risk of inconsistent messages, unsuitable investors or misunderstood risk-return profile.	Approve all investor materials, centralise version control, include risk factors and operate KYC/suitability controls.
Platform-company governance substance	Investors and regulators will test whether Platform Companies have real governance, management, accounts and controls.	Adopt platform board charters, risk registers, delegation matrix and monthly reporting.
Project execution and SPV controls	Housing, healthcare, agro-processing and infrastructure projects can suffer cost overrun, delay, land/title issues and procurement leakage.	Use project gates, feasibility, PMO dashboards, independent monitoring and milestone disbursement.
Healthcare/HMO clinical and claims risk	Healthcare and HMO operations introduce patient safety, provider quality, claims leakage and regulatory risk.	Clinical governance committee, provider due diligence, tariff controls, authorisation rules and claims audit.
Fintech/agency fraud and cyber risk	Agent networks, payments and digital onboarding are vulnerable to fraud, reconciliation failures and data breaches.	AML/KYC, transaction monitoring, agent controls, reconciliation, access management and cyber incident response.
Related-party and intercompany risk	Complex ecosystem can create conflicts, cost-allocation disputes and regulatory perception risk.	Related-party policy, transfer pricing principles, board approvals and transparent registers.
Liquidity and unfunded commitments	Ambitious pipelines can outpace capital availability or create contingent obligations.	Rolling cash forecasts, funding close conditions and commitment approval thresholds.

Appendix C - Regulatory and Technical Reference Anchors

The framework should be reviewed periodically against current Nigerian law, regulator guidance, contractual obligations and sector-specific standards. The following anchors are included for policy alignment and legal/regulatory review; they should not be treated as exhaustive legal advice.

- Investments and Securities Act 2025 - Securities and Exchange Commission Nigeria
- SEC Nigeria - New Rules on Collective Investment Schemes
- Nigerian Code of Corporate Governance 2018
- Nigeria Data Protection Act 2023
- Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024
- NHIA Operational Guidelines 2023
- NHIA Standard Operating Procedure for Claims Submission, Review and Payment
- CBN Payments System Supervision - Guidelines and frameworks
- ICRC PPP Guidelines and Processes
- ISO 31000:2018 Risk Management - Guidelines
- COSO Enterprise Risk Management - Integrating with Strategy and Performance

Closing Institutional Statement

NCDF Group's ability to attract institutional investors, regulators, DFIs, government partners and strategic capital will depend not only on the strength of its opportunity pipeline, but on the credibility of its governance and risk architecture.

This framework provides the Group with a practical and investor-grade operating discipline for controlled growth. It should be implemented as a living system: adopted by the Board, embedded in Platform Companies, translated into risk registers, monitored through KRIs, tested through assurance and continuously improved as the Group expands.