KRESTON PEDABO

Newsletter

September 2026

Welcome to this month's Edition of our newsletter!

As regulation tightens and capital becomes more selective; sustainability, security, and compliance are becoming sources of competitive advantage rather than administrative burdens. This month, we explore how organisations can move from ESG disclosure to genuine integration in **"Embedding ESG for Value Creation: From Compliance to Competitive Advantage."**

We also launch a three-part series, **"The Discipline Gap: Cybersecurity in Africa's Financial Sector,"** examining how digital growth across the continent has outpaced institutional defences.

On tax, **"Impact of The Nigeria Tax Act 2025 on Related Party Financing"** unpacks the new deductibility rules, transfer pricing requirements, and withholding tax changes affecting intercompany financing.

Enjoy your read!

Click on any title to jump to the session

Tyna Adediran
tadediran@krestonpedabo.com
Lead
Management Consulting

Kehinde Folorunsho
kfolorunsho@krestonpedabo.com
Partner
Tax Services

Killian Khanoba
kkhanoba@krestonpedabo.com
Senior Partner
Tax Compliance & Advisory

Albert Folorunsho
afolorunsho@krestonpedabo.com
Managing Consultant

Management Consulting

Embedding ESG for Value Creation: From Compliance to Competitive Advantage

Across markets, the organisations that derive lasting value from environmental, social, and governance (ESG) considerations rarely do so on the strength of disclosure alone. Reporting demonstrates intent, but it is the quality of integration that ultimately determines whether ESG commitments translate into measurable business outcomes. Embedding ESG is precisely that discipline; the systematic, enterprise-wide incorporation of environmental, social, and governance factors into the decisions that shape strategy, capital allocation, and day-to-day operations.

Yet ESG remains widely misunderstood. For many organisations, it is reduced to reporting obligations and reputational management that satisfy external expectations without addressing the structural conditions that determine long-term resilience. True ESG integration is not an annual reporting cycle. It is a management philosophy and an institutional capability that must be embedded into organisational culture, leadership behaviour, and operating systems to generate enduring competitive advantage.

As regulatory expectations tighten and capital becomes more selective across Nigerian and African markets, organisations that invest in building genuine ESG capabilities are better positioned to sustain growth, attract investment, and navigate disruption. Those that continue to rely on narrative disclosure, retrospective data collection, and sustainability functions that sit apart from the core business are finding it progressively harder to satisfy investors, regulators, and international counterparties.

ESG as a Strategic Imperative

The relationship between ESG performance and competitive advantage is increasingly well-established. Environmental exposures influence operating costs and access to resources; social factors affect workforce productivity, customer relationships, and an organisation's licence to operate; and governance weaknesses expose organisations to financial, regulatory, and reputational risk. Organisations that manage these exposures deliberately can protect margin, lower their cost of capital, and respond to regulatory and market change with greater agility. Over time, these capabilities compound into structural advantages that are difficult for competitors to replicate.

The challenge is that ESG integration is not simply a matter of disclosing more or committing more publicly. It requires deliberate investment in the governance structures, data systems, and people capabilities that enable an organisation to identify, measure, and manage the exposures that are material to it. Without this investment, ESG performance tends to be fragile and is easily reversed when reporting deadlines pass or when leadership attention moves elsewhere.

Properly applied, ESG does not displace existing sources of commercial opportunity; it reveals opportunities that were always present but insufficiently examined. The monitoring capability built to support reporting often carries value beyond compliance, as a management tool and occasionally as a commercial proposition in its own right. Organisations with credible sustainability performance are more likely to be favoured by stakeholders in sectors where environmental and social impact is closely scrutinised, and to reach client segments and capital pools operating under explicit sustainability mandates. And the discipline of appraising investments through an ESG lens directs capital towards assets with durable long-term returns and away from exposures likely to become stranded or uneconomic.[1]

As noted in Kreston Pedabo's article on [strategic planning in uncertain times], organisations that maintain clear line-of-sight between enterprise strategy and operational execution are better positioned to allocate resources effectively and adapt to changing conditions. The same logic applies to ESG: organisations that build environmental, social, and governance considerations into standard planning and capital allocation processes accumulate advantages that are compounding and durable.[2]

[1] Henisz, W., Koller, T., & Nuttall, R. (2019). Five Ways that ESG Creates Value. McKinsey Quarterly.
[2] Kreston Pedabo. (2025). Strategic Planning in Uncertain Times: How Businesses Can Stay Ahead.

- Tightening disclosure requirements as Nigeria moves towards mandatory sustainability reporting
- Greater investor scrutiny of climate exposure, governance quality, and social licence to operate
- Financing conditions that increasingly differentiate between issuers on sustainability performance
- Customer and counterparty expectations embedded in procurement and supply chain standards
- Rising energy, water, and raw material costs that reward efficiency and substitution
- The need for credible, auditable data to support access to international capital and markets

In this market, ESG has ceased to be a communications concern. It is a boardroom priority with direct implications for organisational competitiveness, financial performance, and long-term sustainability. The distinction that matters is between compliance, which establishes a floor, and integration, which creates the possibility of differentiation.

The Dimensions of ESG Integration

ESG integration is not a single capability but a set of practices, systems, and behaviours that only produce results in combination. Each of the five dimensions below depends on the one before it: priorities cannot be set without materiality, performance cannot be managed without measurement, measurement cannot be trusted without data infrastructure, none of it operates without capable people, and none of it endures without governance.

Dimension	What it covers	Signal that it is working
Materiality	Identifying the environmental, social, and governance issues capable of affecting the business, and those the business affects	A short, defensible list of priorities that differs by sector
Measurement	Indicators covering emissions, resource use, workforce outcomes, supply chain conduct, and governance effectiveness	Metrics that change management decisions, not just disclosures
Data and technology	Systems, definitions, and collection processes that capture ESG data at source	Figures that can be traced to evidence and withstand assurance
People and capability	Workforce welfare, skills, inclusion, health and safety, and community relationships	Staff who can operate the controls and interpret the data
Governance	Board oversight, defined ownership, review rhythms, and continuous improvement mechanisms	ESG outcomes owned by named people and reviewed on a cycle

Materiality is the entry point, because the ESG priorities of an oil and gas company differ materially from those of a bank, a technology firm, or a manufacturer. It also operates in two directions, asking both whether ESG factors affect the organisation's performance and whether the organisation's activities affect society and the environment. Where both hold, the organisation experiences double materiality and its assessment must reflect enterprise value and external impact alike. Organisations that skip this step tend to address every issue with equal weight, diluting effort and obscuring the exposures genuinely capable of affecting performance.

Once priorities are set, measurement determines whether anything is actually changing. Many organisations track activity rather than outcomes, generate data that is not acted upon, or operate with indicators poorly aligned to their material priorities, which creates the illusion of ESG management without its substance. Credible measurement combines activity metrics, which are captured numerically and support benchmarking, with outcome metrics, which rest on qualitative evidence and are harder to quantify but reveal more about culture and conduct. Both must connect to business outcomes such as resource efficiency, employee retention, risk exposure, and financing conditions. Third-party ratings and certifications then corroborate performance externally, but they are the consequence of sound measurement rather than a substitute for it.

Measurement in turn depends on data infrastructure, and this is where most organisations are weakest. Many understand which issues they ought to monitor but lack the systems to capture them, so reporting rests on estimates rather than evidence. Technology amplifies existing capability, both its strengths and its weaknesses: deployed onto clear data definitions and defined ownership it produces disclosures capable of withstanding assurance, while automating poorly-defined processes simply produces unreliable numbers faster. As highlighted in Kreston Pedabo's article on [navigating the digital landscape](), organisations that integrate technology into well-designed processes are better positioned to compete where digital capability is a baseline expectation rather than a differentiator.[3]

People operate all of it. The social dimension is also, in practice, the one over which organisations exercise the most direct control, encompassing workforce welfare, skills development, inclusion, health and safety, and community relationships. As set out in Kreston Pedabo's article on [building a future-ready workforce](), organisations that invest strategically in capability development are better positioned to sustain performance improvements over time, since framework and system changes are only as effective as the people implementing them.[4]

Governance holds the other four together. Where ownership of ESG outcomes is unclear, initiatives are treated as projects with end dates rather than standing responsibilities, and performance comes to depend on individual conviction rather than institutional discipline. Governance is also what makes improvement continuous, creating the mechanisms through which staff identify exposures, propose interventions, and test them.

[3] Kreston Pedabo. (2024). Navigating the Digital Landscape: Developing a Comprehensive Digital Strategy.
[4] Kreston Pedabo. (2025). Workplace Learning: How to Build a Future-Ready Workforce.

Why ESG Initiatives Often Fall Short

Despite widespread awareness of its importance, ESG integration remains elusive for many organisations. Commitments are announced, initial disclosures are published, and then progress stalls as attention moves elsewhere. Several factors commonly explain the pattern:

- Confining ESG to a dedicated sustainability unit, separated from strategy, finance, risk, and operations
- Leaving competition between short-term commercial targets and longer-term ESG objectives unresolved
- Treating ESG as a reporting obligation rather than a mechanism for managing exposure
- Failing to establish clear ownership of ESG data, metrics, and outcomes
- Pursuing disclosure without the data infrastructure required to make it reliable
- Deferring action in the face of regulatory uncertainty, at an unquantified cost

The most fundamental issue is cultural. ESG is not a technical problem with a technical solution. It is a management discipline that requires sustained leadership commitment, clear accountability structures, and a culture in which the identification of exposures is expected and rewarded rather than treated as an admission of failure. As highlighted in Kreston Pedabo's article on change management strategies, transformation initiatives require deliberate stakeholder engagement, transparent communication, and strong leadership commitment to minimise resistance and support implementation success. This is as true for ESG integration as it is for broader organisational transformation.[5]

[5] Kreston Pedabo. (2024). Change Management Strategies: Overcoming Resistance in Implementation.

Embedding ESG for Sustained Value Creation

The distinction between organisations that achieve temporary improvements in disclosure and those that embed ESG as a durable capability lies in how integration is governed and resourced. It begins at the top. Where boards and senior leaders review sustainability data with the rigour applied to financial data, interrogate the assumptions behind it, and hold executives accountable for outcomes, the signal cascades through the organisation. Commitment of this kind is demonstrated not through public statements but through the questions leaders ask, the information they request, and the standards to which they hold their direct reports.

Ownership must then be explicit at every level. Ambiguity generates gaps in accountability: exposures go unaddressed because no one is clearly responsible for resolving them, and data quality deteriorates because no one owns the source. Establishing ownership requires role clarity, defined indicators, regular review mechanisms that create constructive accountability, and escalation pathways through which ESG issues can be surfaced and resolved.

That ownership only means something if the underlying records will survive examination. Rather than assembling data reactively in the weeks before a reporting deadline, organisations that sustain performance define indicators precisely, document sources and methodologies, retain supporting evidence, and apply the same controls to sustainability information they would to financials. As assurance requirements are phased in, those without an auditable record of how reported figures were derived will struggle to meet them.

Above all, integration has to become part of the standard management rhythm rather than an activity conducted alongside it — regular reviews against clear targets, structured escalation of variances, disciplined follow-through on agreed actions, and periodic reassessment of material issues as the business and its environment evolve.

Kreston Pedabo's ESG IMPACT™ Framework for Embedding ESG into the Core of the Business

To support organisations in moving from ESG commitment to ESG integration, Kreston Pedabo applies the ESG IMPACT Framework: a nine-step model designed to address the structural, cultural, and operational dimensions of sustained ESG performance.

01. Establish
02. Scope
03. Ground
04. Inspect
05. Map
06. Put into Practice
07. Assess
08. Communicate
09. Transform

(E) Establish Governance and Accountability

Ownership of ESG is defined at the organisational level, with the board and senior management setting oversight responsibilities and a cross-functional team coordinating with Finance, Risk, Legal, Operations, and Human Resources.

(S) Scope Material Priorities

The environmental, social, and governance issues most capable of affecting the organisation are identified and prioritised against sector context, concentrating effort where impact is greatest.

(G) Ground the Approach in Relevant Frameworks

The reporting standards relevant to the organisation's objectives and stakeholders are determined, including IFRS S1 and S2, GRI, and SASB where appropriate, selected to support those objectives rather than to dictate them.

(I) Inspect the Current State

Existing policies, practices, controls, data, and performance are assessed against the identified priorities and applicable standards, establishing the distance between where the organisation is and where it needs to be.

(M) Map ESG Objectives to Business Strategy

ESG targets are aligned with commercial objectives and with the organisation's stated purpose, using structured goal-setting disciplines so that targets are specific, measurable, and capable of supporting business planning.

(P) Put ESG into Practice

The actions required to achieve those objectives are determined and assessed for feasibility, cost, potential impact, and fit with existing operations, from energy efficiency and waste reduction to supply chain standards and ethics controls.

(A) Assess Performance and Outcomes

Indicators are established and data is collected and analysed on a regular cycle to determine whether initiatives are producing the intended results, with ESG indicators connected to business outcomes wherever possible.

(C) Communicate Progress and Value

Performance is communicated to stakeholders through sustainability disclosures, annual reports, and other appropriate channels, demonstrating not only what has been done but what has changed and what value has been created.

(T) Transform Through Continuous Improvement

Material issues, regulatory requirements, stakeholder expectations, targets, and performance are periodically reassessed, and the approach is adjusted as the business and the external environment evolve.

This iterating approach ensures that ESG improvements are not only achieved but embedded as a durable organisational capability.

Conclusion

Making ESG Part of How Value Is Created

The organisations that outperform over the long term are rarely those that published the most comprehensive sustainability reports or made the boldest public commitments. More often, they are the organisations that identified what was material to them, integrated it into how decisions are made, and measured the results with the same discipline applied to financial performance.

ESG integration is not a destination but a discipline that must be continuously practised, reinforced, and evolved as the operating environment changes. The organisations that treat it as an institutional capability rather than a reporting obligation are those best positioned to translate commitment into sustained competitive performance.

The imperative for Nigerian and African businesses is clear. In an environment characterised by tightening disclosure requirements, more selective capital, and increasingly demanding counterparties, the ability to demonstrate credible environmental, social, and governance performance is fast ceasing to be a differentiator. It is becoming a prerequisite for long-term viability.

McKinsey has observed that the value of ESG is realised not through the framework itself but through the specific operating decisions it informs: where capital is deployed, how resources are consumed, which markets are entered, and how relationships with regulators, employees, and communities are managed.[12] For organisations ready to act on that, the path is well-understood: rigorous assessment of material exposures, deliberate design of governance and data structures, sustained investment in people capability, and the leadership commitment to hold the organisation accountable for continuous improvement.

For independent advisory support on ESG strategy, materiality assessment, sustainability reporting readiness, and assurance preparation, please contact Kreston Pedabo Management Consulting at:

mc@krestonpedabo.com

[12] Henisz, W., Koller, T., & Nuttall, R. (2019). Five Ways that ESG Creates Value. McKinsey Quarterly.

References

1. Kreston Pedabo. (2025). Strategic Planning in Uncertain Times: How Businesses Can Stay Ahead
2. Kreston Pedabo. (2025). Workplace Learning: How to Build a Future-Ready Workforce
3. Kreston Pedabo. (2024). Change Management Strategies: Overcoming Resistance in Implementation
4. Kreston Pedabo. (2024). Navigating the Digital Landscape: Developing a Comprehensive Digital Strategy
5. Central Bank of Nigeria. (2012). Nigerian Sustainable Banking Principles.
6. Financial Reporting Council of Nigeria. (2018). Nigerian Code of Corporate Governance 2018.
7. Financial Reporting Council of Nigeria. (2026). Roadmap Report for the Adoption of IFRS Sustainability Disclosure Standards in Nigeria (Amendment 2026) and Sustainability Reporting Guideline 1.
8. Henisz, W., Koller, T., & Nuttall, R. (2019). Five Ways that ESG Creates Value. McKinsey Quarterly.
9. Nigerian Exchange Limited. (2019). Sustainability Disclosure Guidelines.
10. Nigerian Exchange Limited. (2024). NGX Impact Board.
11. Securities and Exchange Commission of Nigeria. (2021). Guidelines on Sustainable Financial Principles for the Nigerian Capital Market.

Authors

Khairat Lawal
Intern
Management
Consulting

THE DISCIPLINE GAP

Cybersecurity in Africa's Financial Sector - Part 1 of 3

The Cost of Trust: Cybercrime's New Reality in Nigeria, Ghana, and Beyond

The finance manager at a mid-sized manufacturing distributor in Accra had handled this vendor for three years. So, when an email arrived from the vendor's usual contact, on the vendor's usual letterhead, asking that the next payment go to a "new" account following a "bank migration," there was nothing obviously wrong with it. The tone was right. The invoice number was right. The only thing wrong was the account number, which belonged to a fraudster who had been quietly reading that mailbox's correspondence for weeks. The transfer cleared before anyone thought to pick up the phone. Swap the country, the sector, or the amount, and this story repeats itself across West Africa with almost no variation. It rarely makes the news, because no system was hacked in any technical sense. Nothing was breached. Someone simply lied convincingly, at the right moment, to someone who had no structural reason to doubt them.

That story is the honest starting point for a series on cybersecurity in Nigeria, Ghana, and the wider continent - because the honest picture is less about firewalls and more about how fast this region's digital growth has outrun the discipline needed to defend it.

A Region Running Faster than its Defences

The scale is no longer a matter of anecdote; INTERPOL's most recent continental assessment found that cybercrime now makes up a medium-to-high share of all reported crime in two-thirds of the African countries it surveyed, climbing to roughly 30% of reported crime in Western and Eastern Africa specifically. The same assessment puts cumulative financial losses to cybercrime across the continent at an estimated USD 3 billion since 2019. Phishing, ransomware, business email compromise, and digital sextortion top the list of prevalent threats - and the report is explicit that this is not confined to banks. Attacks on public institutions, including a road transport authority in Kenya and a national statistics agency in Nigeria, show that critical infrastructure is squarely in scope[1].

What that data does not fully capture is the reporting gap underneath it. Most surveyed countries still lack the basic infrastructure; an incident reporting system, a digital evidence repository, a threat intelligence database, to know the true scale of what is hitting them. In practice, this means the number is very likely an undercount, not an exaggeration.

Nigeria: Regulators Are Losing Patience

Nigerian regulators spent the last two years signalling that the era of light-touch enforcement is ending, and 2026 is where that signal became policy. The Central Bank of Nigeria (CBN) introduced a formal Cybersecurity Self-Assessment Tool for financial institutions in March 2026, while the implementing directive under the Nigeria Data Protection Act (NDPA), in force since September 2025, now requires breach notification within 72 hours[2]. Silence is no longer a viable strategy, whatever the reputational instinct to stay quiet after an incident.

Deloitte's Nigeria Cybersecurity Outlook 2026, authored by the firm's Africa Cyber Leader sets out the shape of the year ahead; ransomware and targeted phishing escalating in step with the country's shift to e-invoicing and real-time transaction reporting; a move toward zero-trust, identity-focused security as attackers increasingly steal credentials rather than break through perimeters; intensifying data protection enforcement; heightened risk to government systems as the 2027 election cycle approaches; and a cybersecurity talent gap serious enough that Deloitte cites the ISC2 2025 Cybersecurity Workforce Study's estimate of 4.8 million unfilled cybersecurity roles worldwide as a genuine constraint on how well Nigerian institutions can respond to what is coming[3]. When we have begun to name election-cycle infrastructure risk and workforce shortage in the same breath as ransomware, it is a fair signal that this has moved well past an IT department's problem.

[1] INTERPOL, Africa Cyberthreat Assessment Report 2025 (4th edition, May 2025). Cybercrime accounts for a medium-to-high share of all reported crime in two-thirds of African member countries surveyed, rising to roughly 30% in Western and Eastern Africa; the report estimates USD 3 billion in cybercrime-related financial losses across the continent between 2019 and 2025. Phishing, ransomware, business email compromise, and digital sextortion are identified as the most prevalent threat types, with incidents affecting critical infrastructure including Kenya's Urban Roads Authority and Nigeria's National Bureau of Statistics.

[2] Central Bank of Nigeria, Cybersecurity Self-Assessment Tool for financial institutions, introduced 30 March 2026; and the implementing directive under the Nigeria Data Protection Act (in force since September 2025), which requires regulated entities to notify a breach within 72 hours.

[3] Deloitte Nigeria, Nigeria Cybersecurity Outlook 2026 (Tope Aladenusi, Africa Cyber Leader, Deloitte). The report identifies escalating ransomware and targeted phishing, a shift toward zero-trust and identity-focused defence, accelerating data protection enforcement, heightened risk to government systems ahead of Nigeria's 2027 election cycle, and a widening cybersecurity talent gap, citing the ISC2 2025 Cybersecurity Workforce Study's estimate of 4.8 million unfilled cybersecurity roles worldwide.

Ghana: The Board is Now Explicitly on the Hook

Ghana's regulatory story this year is, if anything, more direct. On 26 March 2026, the Bank of Ghana (BoG) launched its revised Cyber and Information Security Directive (CISD 2026), replacing a 2018 framework the Governor himself described as no longer fit for a 2026 threat environment. CISD 2026 does three things worth noting - it places cybersecurity accountability explicitly at board level, rather than leaving it as a delegated IT matter; it requires regulated institutions to conduct documented due diligence on every third-party vendor and supplier with access to their systems; and it mandates that entities handling card data hold current PCI DSS certification, with methodologies expected to align with NIST and ISO standards[4]. This applies to banks, fintechs, and payment service providers alike, as such the entire financial ecosystem is now under one regime, not a patchwork of exemptions.

That regulatory shift lines up with what CEOs themselves are saying; KPMG's 2025 Global CEO Outlook, surveying 1,350 chief executives, found cybercrime and cyber insecurity ranked as the single largest trend threatening long-term organisational prosperity in banking - cited by 86% of banking CEOs surveyed, ahead of AI workforce readiness and the cost of technology infrastructure. Ghanaian commentary has already picked this up as a direct benchmark for the country's own digitising banking sector[5]. Put plainly, the people running these institutions already know where the risk sits. The Bank of Ghana has now made that knowledge a compliance obligation rather than an internal concern.

Beyond Two Countries

Nigeria and Ghana are not outliers in these trends, they are simply where the data is most visible right now. The same INTERPOL assessment that anchors this piece covers the whole continent, and the pattern it describes - digital adoption outpacing institutional readiness, vendors and third parties as the softest point of entry, public institutions as viable targets alongside banks - shows up wherever mobile money, instant payments, and e-government services have taken hold. The specific sectors and vulnerabilities differ by market; the underlying discipline gap does not. That is exactly the ground the next two pieces in this series will cover in more detail.

[4] Bank of Ghana, Cyber and Information Security Directive (CISD) 2026, launched 26 March 2026 to replace the 2018 framework. The directive places cybersecurity accountability at board level, requires regulated financial institutions to conduct due diligence on third-party vendors and suppliers, mandates PCI DSS certification for entities handling card data, and requires alignment with NIST and ISO information security standards.

[5] KPMG, 2025 Global CEO Outlook, 11th edition (surveying 1,350 CEOs, August-September 2025), as applied to Ghana's banking sector in Ghana-based reporting. Cybercrime and cyber insecurity was ranked by 86% of banking CEOs surveyed as a top trend negatively affecting long-term organisational prosperity, ahead of AI workforce readiness and the cost of technology infrastructure.

A Framework for Reading this Series: KP TRUST™

Every regulator quoted above, in their own way, is describing the same underlying asset under threat; trust - in a bank, in a vendor relationship, in a government record. That is the lens we use internally when we assess an organisation's exposure, and it is the lens this series will keep returning to. We call it TRUST, and it has five parts:

1. **Third-Party & Vendor Exposure:** every vendor, payment gateway, or integration partner that touches your systems or data carries your risk, whether or not you can see their controls.
2. **Reporting Lines & Governance:** whether cyber risk actually reaches the board in a form that supports a decision, rather than a once-a-year dashboard everyone nods at.
3. **Unmapped Attack Surface:** the seams where legacy core systems meet newer digital channels, APIs, and cloud services bolted on over time; this is usually where the real gaps live.
4. **Social Engineering & Human Execution:** how convincingly an attacker can impersonate a trusted colleague, executive, or vendor, and whether your process catches it regardless of how convincing the message is.
5. **Testing & Verification:** whether your controls have actually been tested under real conditions, rather than assumed to work because nothing has gone wrong yet.

We will use these five pillars to structure the rest of this series; the next piece maps specific sector vulnerabilities against them, sector by sector, with the practical controls - including where a targeted penetration test is the fastest way to find out where you actually stand. The final piece turns TRUST into a set of direct questions for CTOs, CROs, CIOs, and CISOs to bring into their next board or audit committee meeting.

The Resulting Situation

None of the regulatory tightening described above is bureaucratic overreach. The Central Bank of Nigeria, NITDA, and the Bank of Ghana are converging on the same conclusion from different directions; that cybersecurity stops being a cost centre inside IT and becomes a standing item of board-level accountability. The institutions that treat this quarter's regulatory changes as the floor, not the ceiling, are the ones that will still be trusted with their customers' money and data when the next Friday-evening email arrives, because by then, someone will have already picked up the phone.

We look forward to sharing Pt 2 of this series.
For enquiries, reach out to mc@krestonpedabo.com

Author

Tyna Adediran
Lead
Management
Consulting

Tax

Impact of The Nigeria Tax Act 2025 on Related Party Financing

Introduction

The Nigeria Tax Act 2025 (NTA 2025) introduces some of the most significant changes to how Nigeria taxes transactions between related or connected companies. As businesses increasingly operate through subsidiaries, affiliates, and group structures, related-party financing — such as intercompany loans, management fees, royalties, and guarantees — has become a major focus for revenue authorities. Under the NTA 2025, the Nigeria Revenue Service (NRS) has been given broader powers to scrutinise these transactions to prevent profit shifting and ensure that tax is paid where economic value is created. Signed on 26 June 2025 and effective from 1 January 2026, the NTA 2025 represents a deliberate shift from the Companies Income Tax Act, Cap C21 LFN 2004 (as amended) (CITA) in how Nigeria taxes financing between related parties. While CITA laid the foundation for taxing corporate profits, NTA 2025 closes gaps that were exploited for profit shifting and aligns Nigeria more closely with global Organisation for Economic Co-operation and Development (OECD) standards.

Related Parties Explained

In accordance with S. 202 of the NTA 2025, “related parties” has the same meaning as connected persons. A company has connected persons where:

I. a person is connected to a company of which he, or his spouse or a close relative has control;
II. a company is connected to another company where the same person has control over both companies, or connected persons acting separately have control over the companies;
III. a company is connected to two or more persons who acting together, or through a person acting on their directions exercise control over the company;
IV. two companies are connected where one company participates directly or indirectly in the management, control or capital of the other company, or the same persons participate directly or indirectly in the management, control or capital of a company and another company.

Related party financing refers to the provision of debt, credit support, or quasi-equity funding between associated entities within a corporate group, typically structured through instruments such as intercompany loans, guarantees, and hybrid securities. Corporate financing is broadly sourced from either equity or debt, with debt obtainable from both independent lenders and related parties. Within multinational enterprises and group structures, related party financing plays a strategic role, reducing reliance on external borrowing, enhancing liquidity management, and facilitating efficient internal capital allocation. Financing of this kind may be obtained from connected parties within Nigeria or abroad.

The applicable accounting standard for related party financing is IAS 24, which requires entities to disclose related party relationships, transactions, and outstanding balances in their financial statements. Its objective is to ensure that financial statements highlight the possibility that an entity’s financial position and profit or loss may have been affected by such relationships.

Stricter Deductibility Rules: An Anti-Profit-Shifting Focus

Beyond its commercial advantages, related party financing carries significant tax implications. It is frequently deployed as a tax planning mechanism, creating opportunities for base erosion and profit shifting (BEPS), particularly through thin capitalisation practices. The fact that interest on debt is generally tax-deductible enables corporate groups to shift profits from high-tax to low-tax jurisdictions. A common concern is that intra-group transactions, which include intercompany loans, licences, and management services, are often mispriced, thereby distorting taxable outcomes, particularly given the potential for profit shifting through excessive interest charges.

The CITA as amended by Finance Act, 2019, introduced an interest deductibility threshold by limiting the tax deductibility of interest on loans from foreign connected persons to 30% of Earnings before Interest, Tax, Depreciation, and Amortisation (EBITDA). Excess interest above this threshold can be carried forward for a period of no more than five years. Under Schedule 3 of the NTA 2025, the scope of transactions subject to the deductibility limitation has been expanded to cover both foreign and local transactions between connected persons, subject to an exemption for companies engaged in banking or insurance. In addition, the definition of debt includes loans, financial instruments, finance leases, and derivatives. The restriction applies broadly to shareholder loans, parent-subsidiary financing, affiliate lending arrangements, and third-party debt guaranteed by related parties, thereby limiting the ability of corporate groups to artificially reduce taxable profits through excessive debt funding.

Transfer Pricing (TP) Documentation and Disclosure Requirements

In line with the provisions of the Income Tax (Transfer Pricing) Regulations 2018, all controlled transactions, including financing arrangements, must comply with the arm's length principle. Accordingly, taxpayers are required to ensure that interest rates, loan tenures, repayment schedules, collateral arrangements, and other financing terms reflect prevailing market conditions. The commercial rationale underpinning any financing arrangement must also be clearly demonstrable and properly substantiated. It is important to carry out transfer pricing analyses and benchmarking studies to ascertain whether a debt financing arrangement is at arm's length. The Comparable Uncontrolled Price (CUP) method is generally the preferred methodology for pricing related party loans, as it benchmarks the interest rate and financing terms against those available in comparable third-party transactions.

Parties that are engaged in related party financing transactions are required to maintain contemporaneous transfer pricing documentation demonstrating compliance with the arm's length principle. Such documentation typically includes executed loan agreements, financial analyses, creditworthiness assessments, benchmarking studies, and evidence establishing the commercial rationale for the financing arrangement.

This is necessary because, under Sections 191 and 192, the Act consolidates the arm's length principle, expands anti-avoidance powers, and equips the tax authorities with direct statutory tools to challenge intra-group arrangements that lack commercial substance or proper documentation. This requires that all related party transactions be conducted on terms and at prices that would prevail between independent parties. There is now stronger statutory backing for transfer pricing adjustments, documentation, and compliance obligations.

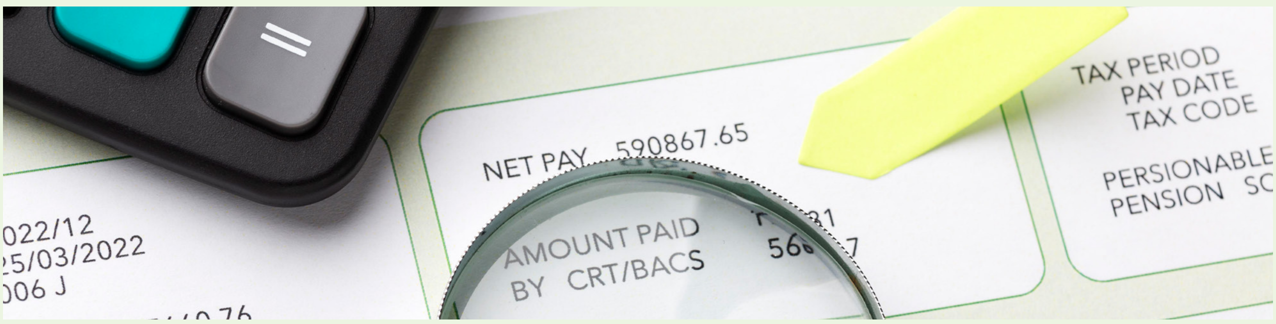
In addition, taxpayers must file the prescribed TP declaration and annual disclosure forms, providing particulars of all related party financing transactions undertaken during the relevant accounting period. This is necessary to avoid penalties and transfer pricing adjustments in respect of non-arm's length transactions.

Interest on Certain Foreign Loans is No Longer Exempt from Withholding Tax

Interest payments arising from related party financing arrangements are generally subject to withholding tax (WHT). The Deduction of Tax at Source (Withholding) Regulations 2024 require the payer of interest to deduct and remit the applicable WHT to the relevant tax authority at the time of payment or when the liability is recognised, whichever is earlier.

The NTA has expunged the previous exemptions of interest payable on certain foreign loans as provided for in Schedule 3 of CITA. Consequently, the tenor, terms or moratorium period of the loan no longer matter. Interest on all foreign loans, including loans from related parties, is now fully subject to WHT in Nigeria at the rate of 10%. The implication is that the cost of accessing foreign debt may increase, and foreign lenders with existing loans in Nigeria may see reduced net yields, which may in turn weigh on the inflow of foreign direct investment into the country.

It should, however, be noted that a reduced rate of 7.5% applies under an applicable double taxation agreement (DTA). As for foreign lenders (which includes foreign related parties), the WHT at the standard rate of 10%, or 7.5% in the case of a lender in a treaty country, will be deducted by the Nigerian borrower and will serve as the final tax liability in line with Section 51 of the Nigeria Tax Administration Act 2025 (NTAA), provided the lender does not have a permanent establishment (PE) or significant economic presence (SEP) in Nigeria.



Conclusion

The Nigeria Tax Act 2025 moves Nigeria closer to global OECD standards. For multinational and domestic groups that use related-party financing, this means increased documentation requirements, tighter controls on interest and fees, and higher audit risk if financing arrangements cannot be justified on commercial grounds. There is therefore a need to ensure that related-party financing is commercially rational, properly priced, and well documented. Groups that proactively review their intercompany loan terms, debt-to-equity ratios, and TP policies will be best positioned to remain compliant.

For enquiries: Taxservices@krestonpedabo.com

Authors

Adewale Kayode
Manager
Tax Srvices

Ayodeji Adenugba
Senior Associate
Tax Services

Esther Nofiu
Senior Associate
Tax Services

Lagos Offices:

67, Norman Williams Street
SouthWest, Ikoyi
Lagos - Nigeria
Tel: 01-2919041; 0808 820 8747

27, Alhaji Bashorun Street
SouthWest, Ikoyi
Lagos - Nigeria

info@krestonpedabo.com
www.krestonpedabo.com

Abuja Office:

Ground Floor, Amb. Albert
Osakwe House
1473, Inner Block Street
Central Business District
Abuja FCT - Nigeria

Tel: 0706 546 89824

Legal Disclaimer:

The material contained in this publication is provided for general information purposes only and does not contain a comprehensive analysis of each item described. Before taking (or not taking) any action, readers should seek professional advice specific to their situation. No liability is accepted for acts or omissions taken in reliance upon the contents of this alert.