SEVENTH EDITION ■ ■ SEP 2026

ACCOBIN
Association of Chief Compliance Officers of Banks in Nigeria
Transparency, Integrity & Ethics

COMPLIANCE DIGEST

NEWS LETTER

INSIGHTS.
PERSPECTIVES.
A STRONGER
COMPLIANCE
COMMUNITY

www.accobin.com.ng

Compliance Starts When Nobody is Watching

COMPLIANCE • ETHICS • TRUST • SUSTAINABLE GROWTH

Contents

SEVENTH EDITION - SEPTEMBER 2026

Building A Culture Of Compliance: MOVING BEYOND POLICIES TO EMPLOYEE OWNERSHIP

Compliance is not a department. It is a decision made hundreds of times a day by employees at every level.

Consider an institution that appears to have done everything right: well-written policies, comprehensive procedures, mandatory training fully attended. And yet a data breach occurs, a suspicious transaction passes unnoticed, confidential information is shared carelessly, a control is bypassed because there was no time. Failure is rarely one of knowledge. Employees knew the rules; they simply did not own them.

In many organisations, compliance is still treated as the responsibility of Compliance, Risk Management, Internal Control or Internal Audit, something done to employees rather than something they contribute to. But frameworks are not sustained by documentation. They are sustained by people making decisions every day. A policy tells an employee what to do; a culture of compliance explains why it matters and gives them the confidence to act when no one is watching.

Where Compliance Actually Lives:

An employee receives an unusual customer request. A colleague suggests skipping a control to save time. Someone considers sending confidential information over an unsecured platform because it is easier. In none of these moments is a Compliance Officer standing nearby. There is only an employee making a decision. Compliance professionals build frameworks and challenge poor practice, but they are almost never the first to encounter a risk. That falls to the people closest to the customer, the process or the transaction.

From Obligation to Ownership

There is a real difference between complying because the policy says so and complying because you understand what is at stake. The first is an obligation; the second is a value. When employees grasp that control protects customers, prevents loss or preserves the organisation's reputation, compliance becomes a matter of judgement rather than an administrative hurdle.

Culture Starts at the Top

Employees watch not only what leaders say, but what they tolerate. When senior staff follow controls even when inconvenient and openly support ethical conduct, the message is clear: this is how we operate. Where targets are consistently prioritised over controls and concerns are quietly dismissed, even a well-designed framework loses its authority.

Make it Practical

Policies are long, regulations technical, training too easily an annual formality. Employees remember compliance when it connects to situations they actually face. Alongside the rule, explain three things: the risk the control addresses, what happens if it is ignored, and what to do when the situation is unclear. That shift from know the rule to understand the risk is what makes compliance usable at the desk.

Recognise Integrity and Make it Safe to Speak Up

Organisations celebrate revenue targets, but rarely the employee who halted a questionable transaction, reported a data exposure or refused a shortcut. Those actions never appear on a dashboard, yet they prevent significant losses. Ownership also requires an environment

where people can raise concerns without fear. Mistakes will happen; the greater danger is silence. A strong compliance culture does not demand perfection it asks people to speak up early.

The Real Measure

The future of compliance will not be defined by thicker manuals or more training modules, but by what employees do when the policy is not in front of them: whether they question what feels wrong, challenge shortcuts, protect customer information unobserved, and report concerns.

Compliance, at its core, is about responsibility making the right decision when no one is standing over your shoulder. When employees stop seeing themselves as subjects of policy and start seeing themselves as owners of the organisation's values, compliance stops being a department's responsibility and becomes an organisation's culture.

Agentic AI and Compliance: Managing Autonomous Decision-Making in Financial Services

For most of the last decade, AI in banking has been about prediction. Models scored credit applications, ranked transaction monitoring alerts, screened names against sanctions lists, and told us how likely something was to be true. The judgement, though, stayed with a person. An analyst read the alert, weighed the context, and decided whether to escalate.

That boundary is dissolving. Agentic AI describes systems that do not just predict but act: they break a goal into steps, call other systems and tools, check their own intermediate results, and carry a task through to completion with limited human involvement. The compliance question has changed. It is no longer whether the model's output is accurate. It is who is accountable when the system acts on it.

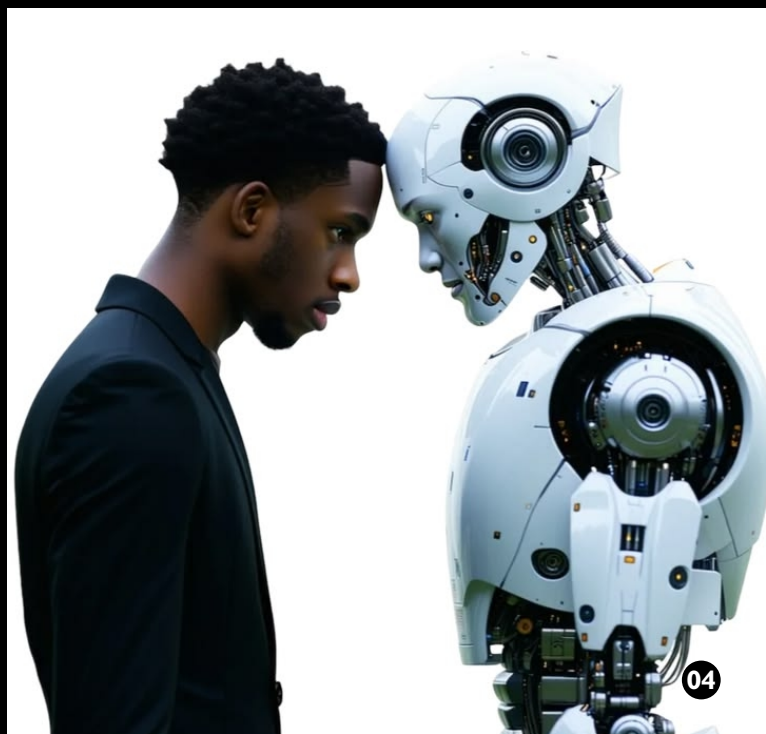
This is not a distant question. Agentic capabilities are already showing up in customer onboarding, service chat, reconciliation and exceptions handling, fraud response, and internal knowledge search. Each of these touches a regulated outcome. A system that can open a case, request a document, adjust a limit, or close an alert is exercising discretion, and one day a regulator will ask us to explain it.

From Assistance to Agency

The practical difference between an assistive model and an agentic one is the length of the chain between the human and the outcome. With an assistive model, the chain is one link: the model recommends, the officer decides. With an agentic system, the chain can run to a dozen steps, several of which leave no trace unless the system was built to log them. It may retrieve a customer record, query an external register, form an intermediate conclusion, act on it, and only show a summary at the end. If one step was wrong, every step after it inherits the error.

The risk is easier to see in a concrete case. Suppose an agent is given a narrow, sensible remit: triage transaction monitoring alerts and prepare case files for investigators. For one alert it pulls the customer record, reads the occupation field as a low-risk category, queries an external register and finds no adverse media, notes that similar patterns on the account were cleared before, concludes the activity is consistent with the customer's profile, and closes the alert as a false positive. Every step is defensible on its own. But the occupation field was three years out of date, and the earlier clearances it treated as precedent were themselves produced by the same flawed reading. What reaches the investigator, if anything does, is a one-line disposition. The error is not in the model's accuracy. It is in the fact that nobody was positioned to catch it.

Our control language was not built for this. It assumes an identifiable maker and an identifiable checker, the four eyes principle. When the maker is a software agent, the checker must be redesigned, not just reassigned.



FROM ASSISTANCE TO AGENCY

How far the human sits from the action

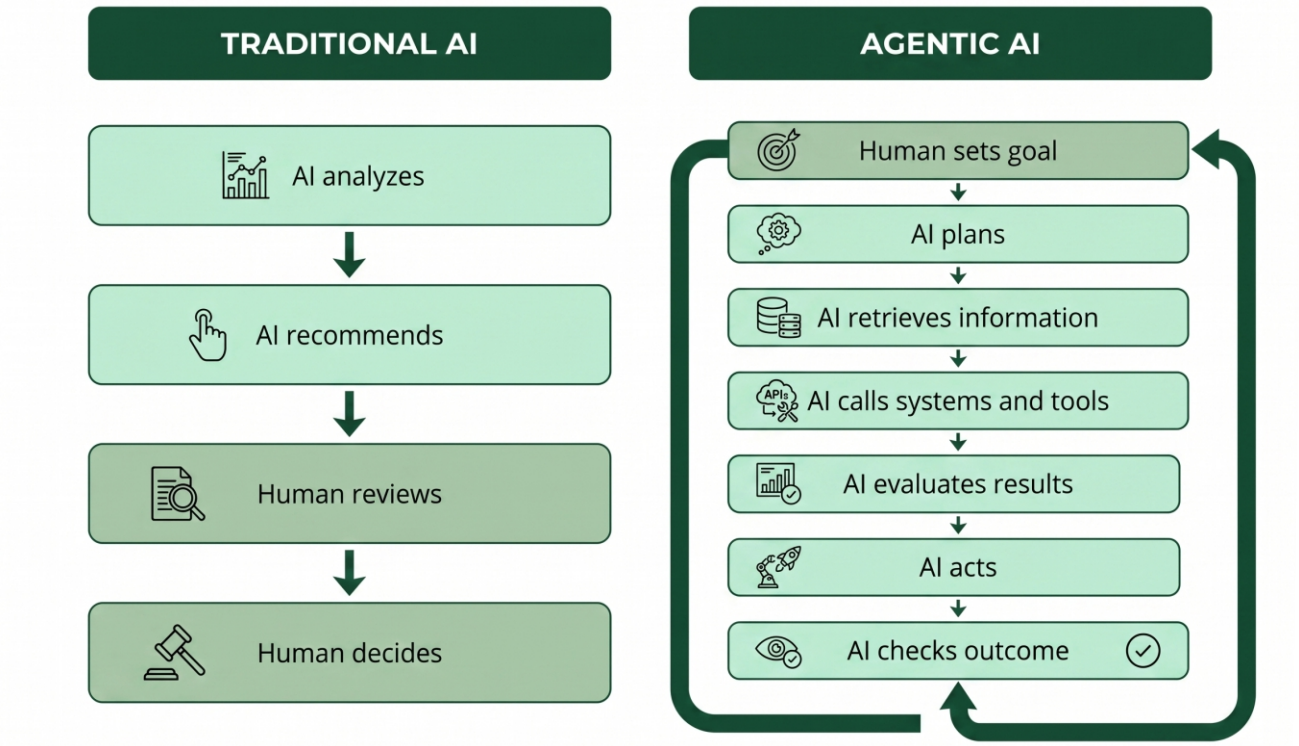


Figure 1: From assistance to agency. Every additional autonomous step lengthens the chain between the human and the action.

Where the Risk Concentrates

Accountability: Responsibility cannot be outsourced, not to a vendor, a subsidiary, or a system. This is a settled principle for the Central Bank of Nigeria (CBN) and international regulators alike, and it applies just as much to Nigeria's own developing AI policy: the National Artificial Intelligence Strategy (NAIS) is built around ethical, accountable adoption, not adoption for its own sake. In practice, this means every agentic deployment needs a named owner in the first line, a defined risk owner, and an approval trail a supervisor can follow from business case to production release.

Explainability: Where an autonomous system contributes to a customer outcome, such as a declined transaction, a restricted account, or an adverse due diligence finding, we must be able to reconstruct the reasoning. Reproducing the final answer is not enough; we need the inputs, the intermediate steps, and the rule or threshold that drove the action. The CBN's 2026 Baseline Standards for Automated AML Solutions elevate this from good practice to binding requirement: institutions using AI or machine learning for transaction monitoring must produce explainable alerts and submit their models for annual independent validation. Immutable, step level logging should be a design requirement from day one, not an afterthought bolted on later.

Data protection: Agentic systems are inherently data hungry; they retrieve, combine, and pass customer information between components to complete a task. The Nigeria Data Protection Act (NDPA) requires a lawful basis, purpose limitation, and data minimization, and a system with broad standing access to customer records sits uneasily against all three. A data protection impact assessment (DPIA) should be a precondition of deployment, and the agent's data access should be scoped to what the task needs, not to whatever the architecture happens to allow.

Drift and silent failure: A conventional control fails loudly; an autonomous system can fail quietly and consistently. If an agent starts closing a category of alerts on a flawed premise, the visible effect is better productivity numbers. Nothing signals a problem until a review, an audit, or a regulatory examination uncovers the pattern. Assurance has to be continuous and outcome based, not a one-time certification at go live.

Third party and concentration risk: Most institutions will acquire agentic capability from a small number of external providers. That puts part of the decision chain outside our direct control. It also puts it inside contractual terms that may not contemplate a Nigerian supervisor's right of access. Contract negotiation, exit planning, and audit rights are compliance matters here, not just procurement ones.

THE AGENTIC AI COMPLIANCE RISK WHEEL

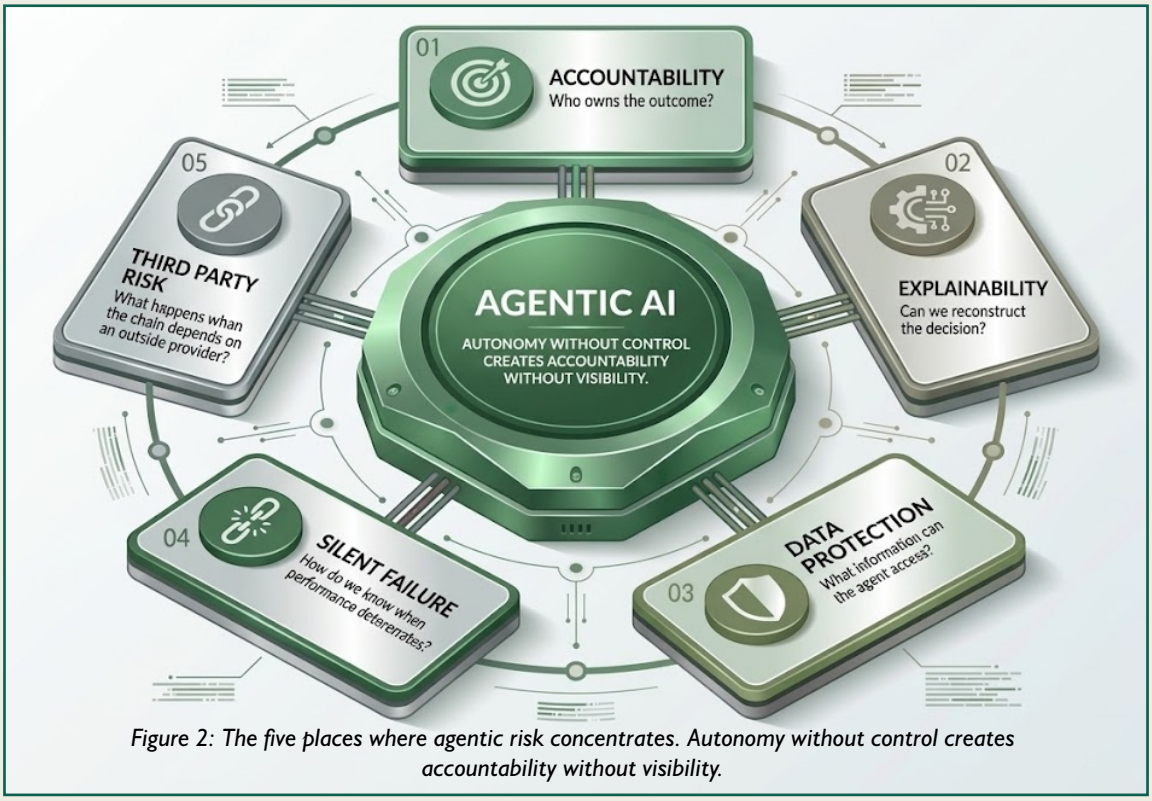


Figure 2: The five places where agentic risk concentrates. Autonomy without control creates accountability without visibility.

A Practical Control Framework

Agentic AI does not require a wholly new rulebook. It needs the disciplined extension of controls we already understand. The table below sets out five domains, the question compliance must be able to answer in each, and the practical control that answers it.

Control Domain	The Question Compliance Must Answer	Practical Control
Ownership	Who is answerable for what this system does in production?	Named business owner and risk owner recorded at approval; included in the risk and control self-assessment (RCSA).
Scope of Autonomy	Which actions may the system take without a human, and which may it never take?	A documented permission boundary with hard coded prohibitions on irreversible or customer adverse actions.
Evidence	Can we reconstruct why the system acted as it did, months later?	Immutable, step level logs of inputs, tool calls, and intermediate conclusions, retained to the record keeping standard.
Data Protection	What personal data does it touch, on what lawful basis, and for how long?	DPIA before go live; least privilege access scoped to the task; a defined retention period.
Ongoing Assurance	How would we know if it started getting things wrong?	Sampled quality review of autonomous outcomes, monitored override rates, and periodic independent testing.

Institutions seeking a readymade structure need not build one from scratch. ISO/IEC 42001, the international standard for AI management systems, maps closely onto the same five domains: ownership and governance, risk assessment, documented controls, data management, and continual monitoring. It is already being adopted by technology providers and financial institutions abroad. Using it as a reference model, whether the bank pursues certification, gives a common language for the conversation with vendors, auditors, and examiners.

Two design principles cut across all five domains. The first is proportionate autonomy: how much freedom an agent has should match how reversible and how customer sensitive the action is. Drafting a summary, retrieving a document, or preparing a case file can safely run on autopilot. Closing a suspicious activity alert, restricting an account, or concluding an enhanced due diligence review should not.

The second is the maintained kill switch. Every deployment needs a tested way to suspend the agent immediately, and a documented fallback to manual processing. The fallback is where most of the work sits: who takes over, how quickly, which cases and transactions are affected, how customers are protected in the interim, and when the regulator has to be told. An escalation path that has never been rehearsed is not a control.

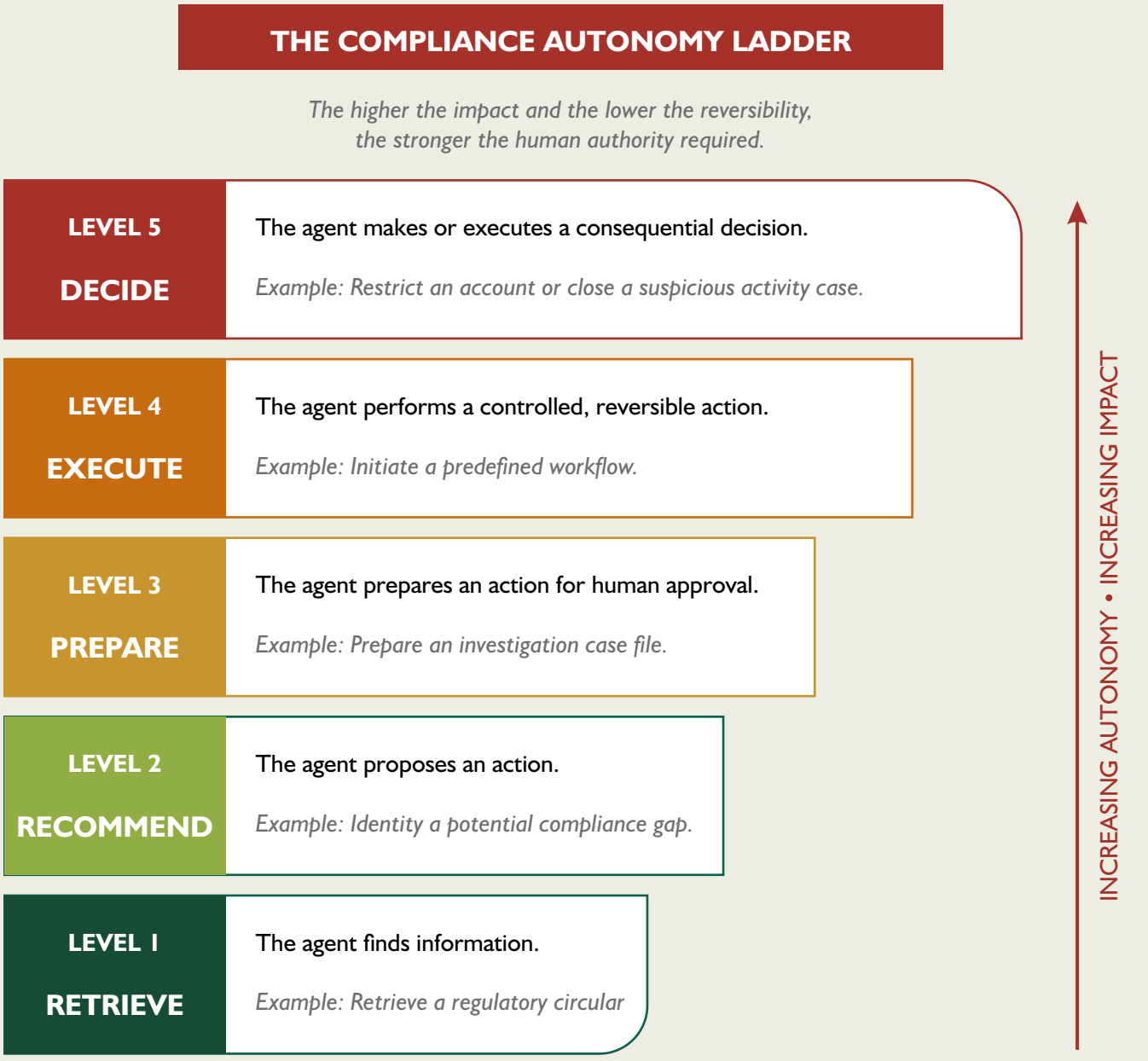


Figure 3: The compliance autonomy ladder. Autonomy is earned level by level; human authority strengthens as impact rises and reversibility falls.

Human Oversight That Is Real

Most governance frameworks respond to automation by inserting a human in the loop. The intention is right, but oversight becomes theatre when the reviewer cannot realistically disagree. If an officer sees hundreds of agent generated conclusions a day, each stated with fluent confidence and none showing its reasoning, approval becomes a reflex. Automation bias is well documented, and volume makes it worse.

The evidence on this is older and starker than the AI debate suggests. In a NASA-funded study of trained glass cockpit pilots, every participant acted on a false automated engine fire alert and shut down a healthy engine, even though other indicators available to them contradicted it. A companion study asked whether a second pair of eyes would help. Two-person crews performed no better than individuals working alone. Four eyes are not a control if both sets are reading the same confident output (Mosier, Skitka, Heers and Burdick, 2000).

Real oversight requires three conditions: the reviewer must have the time, the information, and the standing to disagree. In practice that means workload limits on review queues, interfaces that show the agent's evidence and confidence rather than just its answer, and an escalation route where overriding the system carries no career cost. Compliance should also track the override rate. A rate near zero is not a sign of a perfect model; it is a sign the review has stopped functioning.

Turning the Technology on Compliance Itself

None of this is an argument for caution alone. Compliance is one of the functions with the most to gain. Regulatory change management, reading circulars, directives, and guidelines, and mapping them to internal policy and controls, is exactly the kind of multi-step, document heavy work agentic systems handle well. The same goes for alert triage, adverse media screening, policy gap analysis, and preparing regulatory returns, where the routine work of gathering and reconciling eats time that would be better spent on judgement.

The function that understands the technology will help shape how it is deployed. The function that does not will be handed finished systems and asked to sign off on them. That is the practical case for compliance officers building fluency now, not to become engineers, but to ask the right questions early, while the design decisions are still reversible.

Five Questions Before You Approve

Before signing off an agentic deployment, compliance should be able to answer five questions. If any answer is missing, the deployment is not ready.

- **Who owns the agent?** There must be a namex accountable owner, not a project team.
- **What exactly can it do?** Autonomy needs explicit boundaries, including the actions it may never take.
- **Can we reconstruct everything it did?** If not, the institution may be unable to defend the outcome.
- **What data can it reach?** Access should be task specific and governed by least privilege.
- **What happens when it goes wrong?** There must be monitoring, escalation, a tested kill switch and a manual fallback.

Conclusion

Agentic AI does not introduce a wholly new category of risk. It compresses familiar risks, accountability, explainability, data protection, oversight, third party dependency, into a much shorter timeframe, and removes the natural pauses where human judgement used to step in.

Nigeria's regulatory direction is already aligned with this reality: the CBN's baseline AML standards now require explainability and annual model validation as a condition of using AI in transaction monitoring, and the National AI Strategy sets ethical, accountable adoption as a national goal rather than an afterthought. ISO/IEC 42001 offers a ready structure for institutions that wish to get ahead of both regulatory and supervisory expectations.

Our response must be familiar in principle and more rigorous in execution: clear ownership, autonomy calibrated to impact, evidence captured at every step, oversight genuinely capable of dissent, and

assurance that continues after go live. The institutions that adopt this technology well will not be the ones that move fastest, or the ones that resist longest. They will be the ones that can explain, to a customer or a supervisor, exactly why their system did what it did. That explanation is a compliance product, and building it is our work.

Sources and Further Reading

· Central Bank of Nigeria, Baseline Standards for Automated Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) Solutions, March 2026.

· Federal Ministry of Communications, Innovation and Digital Economy, National Artificial Intelligence Strategy (NAIS), September 2025.

· Nigeria Data Protection Act 2023, and the Nigeria Data Protection Commission's implementing guidance.

· ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.

· K. L. Mosier, L. J. Skitka, S. Heers and M. Burdick, "Automation Bias: Decision Making and Performance in High-Tech Cockpits", International Journal of Aviation Psychology, 8(1), 1998, 47–63.

· L. J. Skitka, K. L. Mosier, M. Burdick and B. Rosenblatt, "Automation Bias and Errors: Are Crews Better Than Individuals?", International Journal of Aviation Psychology, 10(1), 2000, 85–97.

The Future Compliance Professional: **Thriving in a Rapidly Evolving Regulatory Landscape**

> **The compliance profession is at a defining moment. As regulation, technology and business models evolve, the professionals who thrive will be those who combine regulatory expertise with digital fluency, strategic judgement and distinctly human leadership skills.**

The Compliance Profession at a Crossroads

Not long ago, the role of the compliance professional was largely viewed as one of oversight and enforcement. Compliance officers were often perceived as the custodians of regulatory requirements, ensuring that policies were followed, reports were submitted, and breaches were identified. Today, however, that perception is rapidly changing.

The modern regulatory environment is more complex than ever. Financial institutions face an expanding web of obligations covering anti-money laundering, consumer protection, data privacy, cybersecurity, environmental and social governance, artificial intelligence, digital assets, and third-party risk management. At the same time, technological innovation is transforming business models, customer expectations, and the methods regulators use to supervise organisations.

Against this backdrop, compliance is evolving from a traditional control function into a strategic business partner. The compliance officer of the future will not simply interpret regulations; they will help organisations navigate uncertainty, enable innovation, and build sustainable trust.

The question, therefore, is no longer whether the compliance profession will change. The question is whether compliance professionals are prepared for what comes next.

Why the Traditional Compliance Skill Set Is No Longer Enough

The fundamentals of compliance remain important. Regulatory knowledge, integrity, professional scepticism, and risk awareness will always form the foundation of effective compliance management.

However, relying solely on technical regulatory expertise is becoming increasingly insufficient.

Organisations are adopting artificial intelligence to automate routine processes. Advanced analytics are being used to identify emerging risks. Regulatory technology solutions are streamlining monitoring, reporting, and change management activities. Business decisions are increasingly driven by data, and executives expect compliance officers to provide commercially viable solutions rather than simply identify problems.

As a result, the future compliance professional must possess a broader and more dynamic combination of skills. The profession is moving beyond compliance monitoring and into the realms of technology, data analysis, change leadership, and strategic advisory.

Those who embrace this shift will become indispensable business partners. Those who resist it may find themselves struggling to remain relevant in an increasingly digital world.

The Rise of the Digitally Fluent Compliance Officer

Perhaps the most significant transformation affecting compliance today is the growing influence of technology.

Artificial intelligence, machine learning, automated monitoring systems, and regulatory technology platforms are no longer concepts of the future. They are already reshaping the way compliance functions operate. Tasks that once required significant manual effort, such as regulatory change assessments, sanctions screening, transaction monitoring, and report preparation, are increasingly being supported by intelligent systems.

This does not mean compliance professionals need to become software developers or data engineers. However, they must become digitally fluent.

Future compliance leaders will need to understand how technologies work, where their limitations lie, and the risks associated with their deployment. They must be able to challenge assumptions, understand governance requirements, assess potential biases, and ensure that technological solutions operate within established regulatory and ethical boundaries.

In the years ahead, compliance professionals who can confidently engage with technology teams, understand AI-related risks, and participate in digital transformation initiatives will be highly sought after.

Data: The New Language of Compliance

For decades, compliance decisions were often based on policies, experience, and professional judgement. While these remain valuable, the future belongs to evidence-based compliance.

Every day, organisations generate vast amounts of data from customer interactions, complaints, transactions, employee conduct reports, whistleblowing channels, and compliance monitoring activities. Hidden within this information are indicators of emerging risks, control weaknesses, and behavioural trends.

The ability to interpret and analyse data is quickly becoming one of the most valuable skills in the compliance profession.

Tomorrow's compliance professionals must be capable of identifying patterns, recognising anomalies, and transforming information into actionable insight. They will need to understand dashboards, metrics, risk indicators, and analytical tools that support informed decision-making.

In many organisations, the effectiveness of a compliance officer may increasingly be measured not only by the number of issues identified, but also by the ability to anticipate and prevent those issues before they occur.

From Rule Interpreter to Strategic Adviser

A common misconception is that compliance exists solely to enforce regulations. In reality, high-performing compliance functions play a much broader role.

Business leaders increasingly expect compliance teams to support innovation, facilitate growth, and provide practical advice that aligns regulatory requirements with commercial objectives. This requires a shift in mindset.

Future compliance professionals must understand business strategy, operational realities, and organisational objectives. They must be able to evaluate risks in context and recommend solutions that support both compliance and business success.

The most effective compliance officers will not simply say, "No, that cannot be done." Instead, they will say, "Here is how it can be done safely and compliantly."

This ability to balance risk management with commercial awareness will distinguish future compliance leaders from traditional compliance practitioners.

The Human Skills That Technology Cannot Replace

While technology will continue to automate routine compliance activities, certain skills remain uniquely human. Communication is one of them.

Compliance professionals engage with regulators, boards, executives, technology teams, business units, and external stakeholders. Their effectiveness often depends not only on what they know, but also on how effectively they communicate it.

The ability to explain complex regulatory requirements in simple language will become increasingly important. Equally critical is the ability to influence decision-makers, manage conflicting interests, negotiate remediation plans, and build trusted relationships across the organisation.

Empathy, emotional intelligence, and stakeholder management are frequently overlooked competencies, yet they are often the difference between compliance programmes that succeed and those that fail.

Technology may process information faster than humans, but trust is still built through human interaction.

Leadership in an Era of Continuous Change

Regulatory change has become a constant feature of modern business. New regulations emerge regularly, expectations evolve, and organisations are required to adapt quickly.

As a result, compliance professionals are increasingly expected to become change leaders.

Whether implementing a new AML framework, preparing for AI governance requirements, responding to data protection obligations, or adapting to digital asset regulations, compliance teams are often at the centre of organisational transformation initiatives.

Future compliance leaders must therefore understand project management, stakeholder engagement, implementation planning, and change management principles.

The ability to guide organisations through uncertainty will become one of the profession's most valuable competencies.

Looking Ahead: Emerging Areas Every Compliance Professional Should Understand

Several emerging domains are expected to shape the future of compliance over the next decade.

Artificial intelligence governance is rapidly moving up regulatory agendas worldwide, requiring organisations to demonstrate accountability, transparency, and responsible deployment of AI systems.

Environmental, social, and governance considerations are increasingly influencing regulatory expectations and stakeholder scrutiny.
Digital assets, virtual asset service providers, fintech innovations, and decentralised finance ecosystems continue to introduce new compliance risks and regulatory requirements.

Cybersecurity and data protection obligations are becoming more complex as organisations accelerate digital transformation initiatives.

Forward-looking compliance professionals must invest time in understanding these developments before they become mainstream regulatory expectations.

Conclusion: The Compliance Professional of the Future

The compliance professional of the future will look very different from the compliance officer of the past.

While technical regulatory expertise will remain essential, it will no longer be sufficient on its own. Success will require a powerful combination of regulatory intelligence, technological fluency, analytical capability, strategic thinking, communication skills, and ethical leadership.

Artificial intelligence will not replace compliance professionals. It will elevate them.

As routine activities become automated, the value of human judgement, critical thinking, influence, and

leadership will increase. The compliance leaders who thrive in this environment will be those who embrace change, continuously develop new capabilities, and position themselves as trusted advisers rather than regulatory gatekeepers.

Ultimately, the future compliance professional will do far more than ensure compliance with regulations. They will help shape organisational resilience, strengthen stakeholder trust, and contribute directly to long-term business success.

> **In a rapidly evolving regulatory landscape, adaptability may well become the most important compliance competency of all.**

Election Cycles, Financial Crime Risks and the Role of Compliance

Election periods can create a heightened financial crime risk environment for banks. Increased movement of funds for campaigns, logistics, advertising, political engagements, and related activities can create opportunities for money laundering, fraud, bribery, corruption, and illicit political financing.

For financial institutions, particular attention should be given to Politically Exposed Persons (PEPs), campaign sponsors, contractors, intermediaries, and affiliated businesses. Changes in political influence or financial activity may result in transactions that differ significantly from a customer's established profile.

During election cycles, strong KYC, Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and PEP screening become even more important.

Compliance teams should remain alert to:

- Unusual increases in transaction volumes or values.
- Large or unexplained cash movements.
- Transactions inconsistent with a customer's known profile or business.
- Complex third-party payment structures.
- Transactions involving high-risk individuals or entities.
- Unclear beneficial ownership or unexplained sources of funds.

What Should Compliance Teams Do?

Election-related risks should be reflected in the institution's AML/CFT risk assessment and monitoring framework. Compliance teams should consider strengthening transaction monitoring, reviewing high-risk relationships, maintaining effective PEP and sanctions screening, and ensuring timely escalation and investigation of unusual activity.

Importantly, political exposure should not automatically translate into suspicion or adverse treatment. The focus should remain on objective, risk-based assessment and appropriate due diligence.

The Compliance Imperative

Election cycles require Compliance functions to be proactive rather than reactive. Close collaboration across AML, Fraud, Risk, Legal, Operations, and Business teams can help institutions identify emerging risks and respond effectively. Strong compliance controls during election periods help protect banks from financial crime while reinforcing the integrity, resilience, and trustworthiness of the financial system.

The Evolution of Third-Party Risk Management: From Vendor Due Diligence to Continuous Monitoring

The increasing digitalization and interconnectedness of banking have made third parties integral to financial institutions' operations. Banks rely on technology and cloud providers, fintechs, payment partners and other service providers to deliver critical services. But every such relationship extends the bank's risk environment beyond its own walls. A cyber incident, data breach or service disruption at a third party can carry real operational, regulatory and reputational consequences. This raises a fundamental question: can a point-in-time assessment provide sufficient assurance when third-party risk is constantly changing?

From Vendor Due Diligence to Lifecycle Management

Traditionally, third-party oversight followed a simple model: identify a vendor, run due diligence, approve, contract and onboard. The focus was largely on whether a prospective vendor was credible, financially sound and compliant. That Due Diligence remains a fundamental control, but it only ever captures a snapshot. A vendor that looks sound at onboarding may later face a change in ownership, weakened financials or a slipping security posture. This has driven a shift from asking " Is this vendor acceptable?" to asking "What risks does this relationship introduce, and how do we manage them across its lifecycle?" Modern Third-Party Risk Management now applies a risk-based, lifecycle approach that runs from identification and classification through contracting, onboarding, monitoring, reassessment and eventual exit, with the depth of scrutiny calibrated to a vendor's criticality, access and substitutability. Due diligence becomes one component of this continuous process rather than its endpoint, and the emphasis moves from simply collecting documents to ensuring that controls are actually implemented and effective.

Continuous Monitoring: The New Frontier

Continuous monitoring sits at the heart of this evolution. It provides ongoing visibility into changes in a third party's regulatory standing, cybersecurity posture, financial condition, service performance and ownership. Effective monitoring combines scheduled reviews with event-driven reassessment, so that a material breach, regulatory action or **SLA** failure, triggers immediate review rather than waiting for the next cycle. The risk perimeter must also extend beyond the immediate vendor to fourth-party and supply-chain risks, particularly where critical providers depend on other service providers for technology, cloud infrastructure or other essential services. This is ultimately about resilience as much as prevention. Institutions need business continuity plans, tested exit strategies and clear escalation paths for when something goes wrong, underpinned by shared ownership across Procurement, Compliance, Information Security, Legal and the Board.

A Regulatory Anchor

This trajectory aligns with regulatory direction both locally and globally. The CBN IT Standards Blueprint emphasizes risk assessment and due diligence covering areas such as reputation, internal controls, financial performance and business continuity, while recognizing that reliance on service providers does not remove the financial institution's responsibility for managing the associated risks. The Basel Committee's 2025 principles similarly push banks beyond traditional outsourcing oversight towards lifecycle-based third-party risk management, with particular attention to criticality, supply-chain and concentration risks. Increasingly, technology, data analytics and AI-enabled capabilities may help make continuous risk intelligence more scalable and responsive.

Conclusion

The journey is clear. It moves from vendor due diligence to risk-based assessment, then to lifecycle management, then to continuous monitoring, and ultimately to continuous risk intelligence. The objective is no longer simply confirming that a vendor was acceptable at onboarding, but maintaining current assurance that the relationship stays within the institution's risk appetite throughout its life. The question has evolved from "have we completed due diligence?" to "has anything changed that requires us to reassess?" That is the evolution from vendor due diligence to continuous monitoring.

From "Situationship" to Structured Governance: The Imperative of Explicit Consent in Data Protection.

Have you ever found yourself in what felt like a relationship, yet there was no clear proposal, no defined expectations, and no assurance of commitment? There were activities, assumptions, and emotional investments, but no clarity, no boundaries, and no mutual understanding. In contemporary language, such an arrangement is often described as a "situationship."

While this analogy may appear light-hearted, it provides a powerful lens through which we can examine governance failures in business relationships, particularly in the area of data protection and privacy compliance.

The Governance Lesson: Clarity Before Commitment

In personal relationships, the absence of clarity breeds confusion, unmet expectations, and avoidable harm. The same principle applies to corporate engagements, especially when organizations collect and process personal data.

When customers open accounts, subscribe to services, or engage with digital platforms, they enter into a formal relationship with an organization. That relationship carries legal and regulatory obligations. Under the **Nigeria Data Protection Act (NDPA) 2023,** enforced by the Nigeria Data Protection Commission, organizations are required to obtain **clear, specific, and explicit consent** for defined purposes of data processing. Implied consent is no longer sufficient for activities such as:

- Email marketing communications
- Automated decision-making
- Profiling activities
- Sharing or transferring data to third parties
- Cross-border data transfers (where applicable)

Simply filling out a form to initiate a service relationship does not automatically authorize the organization to process personal data for all ancillary purposes.

From Assumptions to Accountability

Just as boundaries define healthy personal relationships, transparency defines compliant corporate relationships.

Organizations acting as Data Controllers or Data Processors must:

- Clearly state the purposes for data collection
- Identify the lawful basis for processing
- Explain data subject rights
- Outline data retention timelines
- Disclose third-party sharing arrangements
- Provide accessible and understandable privacy notices

Failure to do so moves the organization from structured compliance into a regulatory "situationship" one characterized by ambiguity, exposure, and enforcement risk.

The Role of Assurance Team

For the Data Protection Officer, Compliance, and Internal Audit Functions, this presents a critical assurance responsibility.

Assurance team should assess:

- Whether consent mechanisms are granular and purpose specific.
- If privacy notices are updated, accessible, and legally aligned.
- Whether consent withdrawal processes are operational and effective.
- If marketing and automated decision systems rely on lawful consent records.
- Whether governance frameworks reflect NDPA obligations.

Data protection compliance is not merely a legal issue; it is a governance, risk, and control matter. Weak consent frameworks expose organizations to regulatory sanctions, reputational damage, and erosion of stakeholder trust.

While organizations must uphold regulatory standards, individuals also bear responsibility for understanding their privacy rights.

Reading privacy policies before consenting may not yet be a widespread habit, but informed stakeholders strengthen accountability ecosystems. An aware customer base reinforces better governance practices.

In an era of increasing digital interdependence, transparency must replace assumption, and consent must replace implication.

In governance, as in relationships, clarity precedes commitment.

The transition from "situationship" to structured, accountable engagement requires:

- Explicit consent
- Transparent communication
- Defined boundaries
- Ongoing oversight

When consent is explicit and transparency is embedded, organizations move from regulatory vulnerability to institutional integrity.

Stay Informed.

Stay Compliant.

Strengthen Governance.

Blessing Ejike
Data Protection
Topic: *Building a Culture of Compliance: Moving Beyond Policies To Employee Ownership.*

Adeyemi Olupeka
Compliance Risk Management
Topic: *Agentic AI and Compliance: Managing Autonomous Decision-Making in Financial Services.*

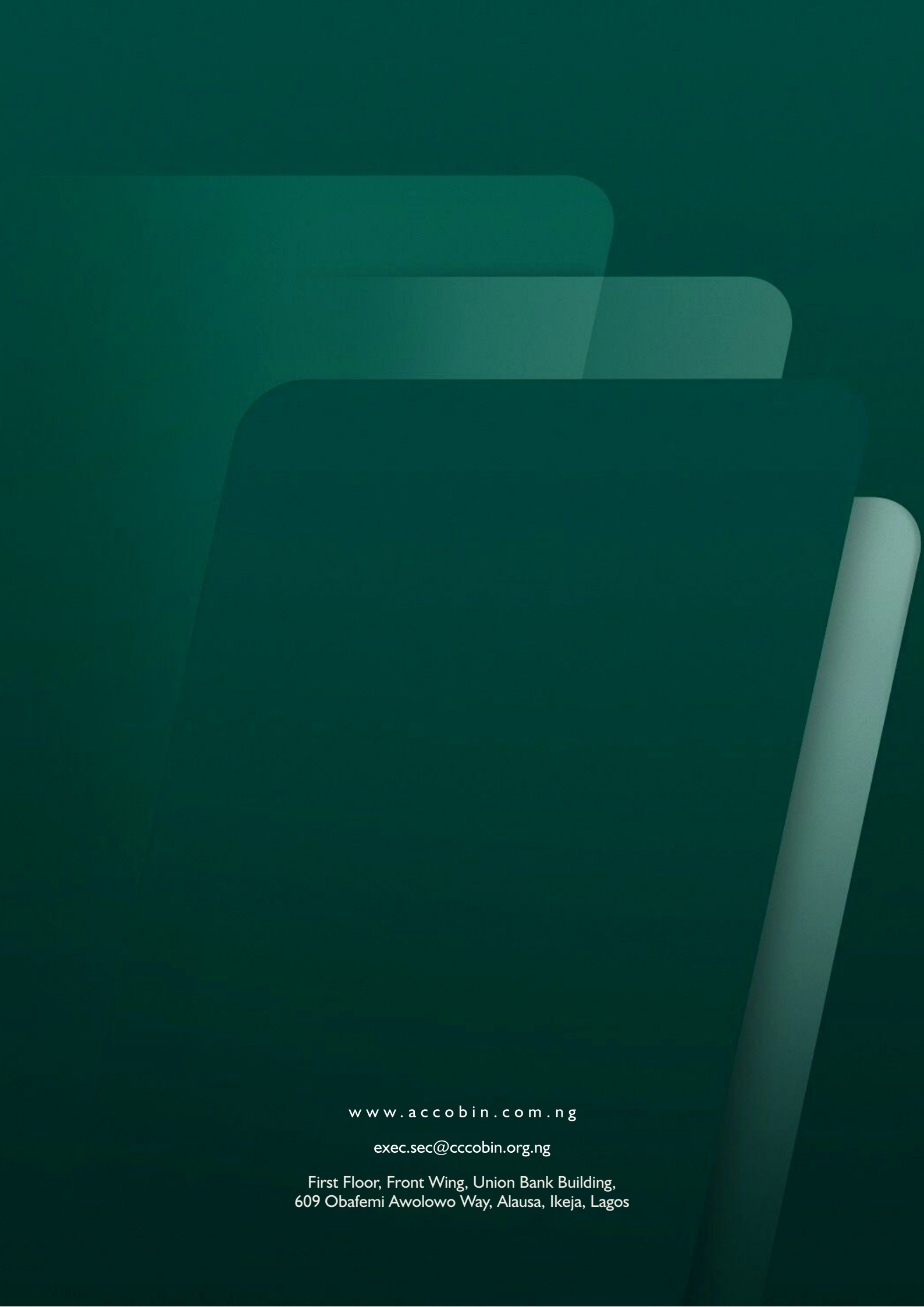
Oghenetejiri Gbemre
Topic: *The Future Compliance Professional: Thriving in a Rapidly Evolving Regulatory Landscape.*

Ganiyat Quadri
Compliance Risk Management
Topic: *Election Cycles, Financial Crime Risks and the Role of Compliance.*

Beauty Orisabinone
Compliance Risk Management
Topic: *The Evolution of Third-Party Risk Management: From Vendor Due Diligence to Continuous Monitoring.*

Stella Okeke
Data Protection and Privacy
Topic: *From "Situationship" to Structured Governance: The Imperative of Explicit Consent in Data Protection.*

All contributors are staff of Fidelity Bank.



www.accobin.com.ng

exec.sec@cccobin.org.ng

First Floor, Front Wing, Union Bank Building,
609 Obafemi Awolowo Way, Alausa, Ikeja, Lagos