SPEECH BY THE DIRECTOR-GENERAL/CHIEF EXECUTIVE OFFICER OF THE NATIONAL IDENTITY MANAGEMENT COMMISSION (NIMC)

ENGR. (DR.) ABISOYE COKER-ODUSOTE

AT THE ICAN EVENT

PLENARY SESSION: DIGITAL GOVERNANCE — LEVERAGING TECHNOLOGY FOR ACCOUNTABILITY AND TRANSPARENCY

PROTOCOL

Distinguished Chairman of this Session,
Esteemed Members of the High Table,
President and Members of the Institute of Chartered Accountants of Nigeria (ICAN),
Distinguished Fellows and Members of the Institute,
Representatives of Government Institutions,
Distinguished Policymakers, Industry Leaders,
Ladies and Gentlemen.

I bring you warm greetings from the Director-General/Chief Executive Officer of the National Identity Management Commission, Engr. (Dr.) Abisoye Coker-Odusote, who sends her regards and appreciates the opportunity to contribute to this important conversation.

It is a great honour to address this distinguished gathering on a subject that is central to the future of public administration, institutional effectiveness and national development: **Digital Governance—Leveraging Technology for Accountability and Transparency.**

I commend ICAN for providing this important platform to discuss how technology can strengthen public institutions, improve financial accountability, enhance transparency and build public confidence in governance.

In an increasingly interconnected world, digital governance is no longer simply an option for governments seeking to modernise their operations. It is an essential foundation for effective service delivery, institutional integrity, economic growth and national transformation.

For Nigeria, the opportunity before us is significant. By strategically deploying technology, strengthening digital identity infrastructure and promoting data-driven decision-making, we can build public institutions that are more transparent, efficient, accountable and responsive to the needs of our citizens.

As Director-General and Chief Executive Officer of the National Identity Management Commission, I will share perspectives on the role of digital identity in advancing accountable governance, the importance of technology in public-

sector financial management, and the opportunities available to Nigeria as we continue our journey towards a more digitally enabled government.

1. UNDERSTANDING DIGITAL GOVERNANCE

Digital governance goes beyond the computerisation of government processes. It involves the deliberate use of digital technologies, trusted data, secure systems and integrated platforms to improve the way government institutions operate, make decisions, manage resources and serve citizens.

It requires a fundamental shift from fragmented, paper-based processes to connected, transparent and data-driven systems.

In traditional administrative environments, the delivery of public services can be slowed by manual procedures, duplicated records, fragmented databases, limited information sharing and inadequate monitoring mechanisms. These weaknesses can create opportunities for inefficiency, revenue leakages, fraud and poor accountability.

Digital governance provides practical solutions to these challenges.

Through automation, secure information exchange, electronic records, digital payments, data analytics and real-time monitoring, government institutions can strengthen internal controls, reduce administrative bottlenecks and improve the traceability of decisions and transactions.

However, technology alone does not guarantee good governance. Its effectiveness depends on strong institutions, sound policies, competent personnel, effective oversight and a culture of integrity.

The objective, therefore, is not merely to digitise existing processes, but to redesign them in ways that promote transparency, enforce accountability and deliver measurable public value.

2. DIGITAL IDENTITY AS THE FOUNDATION OF TRUSTED GOVERNANCE

At the National Identity Management Commission, we recognise that a trusted national identity system is one of the foundational pillars of digital governance.

A government cannot effectively deliver services, implement social protection programmes, prevent identity-related fraud or maintain accurate public records without reliable mechanisms for establishing and verifying the identity of individuals.

Digital identity helps answer a fundamental question in governance: **How can government confidently establish who is accessing a service, receiving a benefit or participating in a transaction?**

Nigeria's National Identification Number, or NIN, provides an important foundation for answering this question.

The NIN enables identity verification across multiple sectors, supporting financial services, telecommunications, public administration, social intervention programmes and other services where reliable identity information is required.

As at October 2026, Nigeria's national identity programme has recorded approximately **143 million enrolments and 123 million NIN issuances**, reflecting the scale of progress in building a comprehensive national identity infrastructure.

These achievements represent more than numbers. They demonstrate the growing capacity of the country to establish trusted identity records that support inclusion, service delivery and institutional coordination.

Nevertheless, enrolment is only one part of the journey. The greater opportunity lies in using trusted identity infrastructure responsibly to improve governance outcomes.

This requires accurate data, strong authentication mechanisms, secure interoperability and clear rules governing access to identity information.

3. NINAuth: ADVANCING TRUSTED DIGITAL IDENTITY AUTHENTICATION

One of the important developments in Nigeria's digital identity ecosystem is the National Identification Number Authentication Service, known as **NINAuth**.

NINAuth provides a unified platform for trusted digital identity authentication, enabling authorised organisations to verify identity through a more structured and secure framework.

The importance of such a platform becomes clearer when we consider the challenges associated with fragmented verification arrangements, inconsistent integration methods and limited visibility across service channels.

A unified authentication framework can help improve consistency, strengthen identity assurance and support better coordination among authorised stakeholders.

For financial institutions, identity authentication can strengthen customer verification and support efforts to combat identity fraud.

For telecommunications operators, it can support identity-related compliance and verification requirements.

For government agencies, it can improve confidence in identity-dependent services and help strengthen the integrity of administrative processes.

For authorised security agencies, appropriately governed access to authentication services and relevant dashboards can support investigations, identify patterns of suspicious activity and strengthen inter-agency collaboration, subject to applicable legal authority and access controls.

NINAuth also offers an opportunity to promote greater inclusion by helping organisations build services around a trusted identity framework rather than maintaining unnecessary, disconnected verification arrangements.

However, we must be clear that trusted authentication must be accompanied by robust cybersecurity, appropriate privacy safeguards, clear accountability for access and responsible use of personal data.

Our objective is to ensure that digital identity strengthens public trust rather than creating new risks to citizens' privacy or security.

4. TECHNOLOGY AS AN INSTRUMENT OF FINANCIAL ACCOUNTABILITY

The theme of this engagement is particularly relevant to the accounting profession.

Accountability requires institutions to demonstrate how resources are collected, allocated, spent and reported. Transparency requires that appropriate information is accessible, verifiable and available to authorised oversight bodies.

Technology can strengthen both objectives.

First, digital financial management systems improve transaction traceability. Electronic records can provide audit trails showing when a transaction occurred, who initiated or approved it, and whether the relevant control procedures were followed.

Second, automated workflows can enforce segregation of duties. A person initiating a payment, for example, should not automatically have unrestricted authority to approve and reconcile that same transaction.

Third, integrated financial and administrative systems can reduce duplication, improve data consistency and make it easier to reconcile transactions across departments and institutions.

Fourth, analytics and automated exception reporting can help auditors and financial managers identify unusual transactions, duplicate payments, unexplained variations and potential control weaknesses earlier.

Fifth, digital dashboards can provide management and oversight bodies with timely information on expenditure, revenue, procurement, project implementation and institutional performance.

These capabilities can move accountability from a largely retrospective exercise to a more continuous process of monitoring, prevention and intervention.

Rather than discovering every control failure only after the end of a financial year, institutions can increasingly identify exceptions as they arise and respond before losses escalate.

For ICAN and the wider accounting profession, this transition presents an important opportunity to strengthen the contribution of accountants to public-sector governance.

The accountant of the digital age must be more than a custodian of financial records. The profession must increasingly serve as a strategic partner in data

governance, technology assurance, risk management and institutional performance.

5. DIGITAL IDENTITY AND THE PREVENTION OF FRAUD

One of the most important contributions of trusted identity infrastructure is its potential to reduce identity-related fraud and improve the integrity of public programmes.

Where identity records are unreliable or verification processes are fragmented, institutions may struggle to establish whether an individual is entitled to a benefit, whether records refer to the same person or whether an identity is being used improperly.

These weaknesses can affect social intervention programmes, public-sector payrolls, pension administration, financial services and other identity-dependent activities.

A reliable identity framework can help authorised institutions verify individuals, improve record matching and reduce the risk of duplicate or fraudulent claims.

Nevertheless, identity verification should be understood as one component of a broader control framework. It does not, by itself, establish entitlement to a payment or prove that every transaction is legitimate.

Effective fraud prevention requires identity assurance to be combined with sound business rules, financial controls, independent audits, secure information exchange and effective investigation.

This is where collaboration between identity institutions, accountants, auditors, financial regulators, law-enforcement agencies and other public institutions becomes especially important.

By combining reliable identity verification with appropriate financial and administrative controls, Nigeria can strengthen the integrity of public expenditure and improve confidence in government programmes.

6. INTEROPERABILITY AND A CONNECTED GOVERNMENT

A major challenge facing public administration is the fragmentation of information across institutions.

Different government agencies often maintain separate systems to support their respective mandates. While such systems may be necessary for specialised operations, the absence of appropriate interoperability can create duplication, increase costs and make coordinated service delivery more difficult.

Digital governance requires a more connected approach.

Interoperability allows authorised systems to exchange relevant information securely, using agreed standards, protocols and governance arrangements.

The objective is not to create unrestricted access to every government database. Rather, it is to enable lawful, controlled and purpose-specific information exchange.

Nigeria's digital public infrastructure must increasingly support collaboration among identity management, financial administration, taxation, telecommunications, social protection and other public services.

Such integration can help institutions validate information more efficiently, reduce repeated data collection and improve the consistency of administrative records.

However, interoperability must be supported by clear data ownership, defined institutional responsibilities, access controls, audit logging and mechanisms for resolving data-quality issues.

We must build a government in which information can move securely where it is legitimately required, without compromising the rights of citizens or the responsibilities of individual institutions.

7. CYBERSECURITY, PRIVACY AND RESPONSIBLE DATA GOVERNANCE

As government becomes increasingly digital, the importance of cybersecurity and data protection cannot be overstated.

Digital systems create enormous opportunities, but they also expose institutions to cyberattacks, data breaches, insider threats, service disruptions and the misuse of sensitive information.

The more interconnected our systems become, the more important it is to protect them through a comprehensive security framework.

At NIMC, protecting the integrity, confidentiality and availability of identity information is central to our responsibilities.

This requires continuous security monitoring, robust identity and access management, secure system architecture, incident response capabilities, disaster recovery arrangements and regular assessment of security controls.

The establishment and strengthening of Security Operations Centre capabilities, for example, supports improved monitoring, threat detection and coordinated responses to cybersecurity incidents.

Equally important is the principle that access to personal information must be lawful, necessary, proportionate and appropriately controlled.

Public confidence in digital governance depends not only on whether systems work, but also on whether citizens believe their information is being handled responsibly.

We must therefore embed privacy and security into the design of digital systems from the outset, rather than treating them as additions after implementation.

Strong governance arrangements must also define accountability for data access, retention, sharing and disposal, alongside appropriate procedures for investigating misuse.

Digital trust is an institutional asset. It must be earned, protected and continually reinforced.

8. THE ROLE OF ARTIFICIAL INTELLIGENCE AND DATA ANALYTICS

Artificial intelligence, machine learning and advanced analytics are creating new opportunities to improve public administration.

These technologies can support anomaly detection, risk assessment, demand forecasting, fraud identification and more effective allocation of resources.

In financial management, analytics can help identify unusual spending patterns, potential duplicate transactions and emerging budgetary pressures.

In public service delivery, predictive analysis can help institutions anticipate demand, identify service bottlenecks and allocate resources more efficiently.

In identity management, carefully governed analytical tools can support data-quality assessment, system performance monitoring and the detection of suspicious patterns.

However, the adoption of artificial intelligence must be guided by responsible governance.

Automated systems must not become unaccountable decision-makers. Their outputs should be subject to appropriate human oversight, validation, documentation and review.

Institutions must also address the risks of inaccurate data, algorithmic bias, unauthorised access and decisions that cannot be adequately explained.

The objective is to use technology to strengthen professional judgement and institutional capability, not to eliminate responsibility for decisions.

For accountants and auditors, these developments make technology literacy, data analytics and digital assurance increasingly important professional competencies.

9. BUILDING DIGITAL CAPACITY AND INSTITUTIONAL READINESS

No digital transformation programme can succeed through infrastructure alone.

The success of digital governance depends on people, processes, leadership and institutional culture.

Government institutions must invest in the skills required to design, implement, secure, operate and audit modern digital systems.

This includes capacity in cybersecurity, software engineering, database administration, cloud infrastructure, data analytics, digital forensics, technology risk management and information governance.

At the same time, public servants must understand how digital processes affect their responsibilities, decision-making authority and accountability obligations.

Change management is therefore essential.

Institutions must establish clear ownership of digital transformation initiatives, measurable implementation milestones, sustainable funding arrangements and performance indicators linked to actual service outcomes.

Procurement decisions must be guided by value for money, interoperability, security, sustainability and the total cost of ownership, rather than acquisition cost alone.

We must also avoid creating digital systems that simply reproduce inefficient manual processes in electronic form.

True transformation requires us to examine existing procedures, remove unnecessary bottlenecks, strengthen controls and redesign services around the needs of citizens and institutions.

10. THE STRATEGIC IMPORTANCE OF THE NEW NIMC ACT

The National Identity Management Commission's mandate is also evolving within the context of the new NIMC Act, 2026.

The Act provides an important framework for strengthening the Commission's role in Nigeria's national identity management ecosystem and advancing the strategic use of trusted identity infrastructure.

As the Commission implements its expanded responsibilities, effective coordination with relevant government institutions, regulators, technical partners and other stakeholders will be essential.

A key strategic area is the transition towards a stronger national Public Key Infrastructure and the associated Root Certification Authority arrangements, in line with the applicable legal and institutional framework.

Public Key Infrastructure provides mechanisms for establishing digital trust through cryptographic certificates, authentication, digital signatures and the validation of electronic transactions.

When properly implemented and governed, these capabilities can support more secure digital interactions, strengthen document integrity and provide a foundation for trusted electronic services.

They can also complement digital identity authentication by helping institutions verify the authenticity and integrity of electronic communications and transactions.

Our focus must be on establishing a sustainable, secure and well-governed national digital trust ecosystem, with clearly defined institutional responsibilities, appropriate technical standards and effective oversight.

This work forms part of the broader effort to ensure that Nigeria's digital public infrastructure is not only functional but also trusted, resilient and capable of supporting the country's long-term development objectives.

11. THE ACCOUNTING PROFESSION AS A PARTNER IN DIGITAL GOVERNANCE

Distinguished ladies and gentlemen, the accounting profession has a vital role to play in Nigeria's digital transformation.

Accountants and auditors possess the professional expertise required to evaluate the financial implications of technology investments, assess internal controls, examine transaction records and determine whether public resources are being used efficiently.

As government systems become more digital, the profession must evolve to address new forms of risk and new opportunities for assurance.

This includes evaluating the integrity of digital records, assessing automated financial controls, reviewing access permissions, examining system-generated audit trails and understanding the risks associated with artificial intelligence and third-party technology providers.

ICAN can make an important contribution by promoting continuous professional development in digital accounting, information systems auditing, cybersecurity awareness, data analytics and technology risk management.

There is also an opportunity to strengthen collaboration between accounting professionals and technology specialists in the design and assessment of public-sector systems.

Financial accountability should not be considered only at the point where expenditure is reported. It should be built into the architecture of the systems through which public resources are managed.

When financial controls, auditability and transparency are incorporated from the beginning, institutions are better positioned to prevent irregularities, demonstrate compliance and provide credible reports on performance.

I therefore encourage ICAN and its members to continue engaging actively with government institutions in shaping the policies, standards and professional capabilities required for responsible digital governance.

12. CHALLENGES AND THE WAY FORWARD

Despite the progress Nigeria has made, several challenges require sustained attention.

These include legacy infrastructure, fragmented databases, uneven digital capacity, cybersecurity threats, inadequate funding for maintenance, resistance to institutional change and the need for stronger coordination across government.

Addressing these challenges requires a practical and coordinated approach.

First, we must strengthen digital infrastructure and ensure that critical systems have appropriate resilience, backup and disaster recovery capabilities.

Second, we must establish and enforce common standards for interoperability, data quality, cybersecurity and information governance.

Third, we must strengthen institutional accountability by assigning clear responsibilities for technology investments, operational performance and risk management.

Fourth, we must invest in people through targeted training, professional development and the retention of critical technical expertise.

Fifth, we must measure digital transformation by its outcomes. Success should be assessed through improved service delivery, reduced processing times, better financial controls, stronger security, lower operational costs and increased public confidence.

Finally, we must sustain collaboration among government institutions, professional bodies, the private sector and development partners.

Digital governance is a collective responsibility. No single institution possesses all the capabilities required to deliver it.

13. CONCLUSION: BUILDING A TRUSTED AND ACCOUNTABLE DIGITAL NIGERIA

Distinguished ladies and gentlemen, the future of governance will increasingly depend on our ability to use technology responsibly to strengthen institutions, protect public resources and improve the lives of citizens.

Digital identity provides a foundation for trust. Interoperability enables collaboration. Cybersecurity protects our systems. Data analytics improves decision-making. Digital financial management strengthens accountability. Professional standards ensure that these capabilities are deployed responsibly.

But the ultimate measure of success is not the number of systems we deploy or the volume of data we process.

It is whether our citizens receive better services, whether public resources are managed more transparently, whether fraud becomes more difficult to perpetrate, whether institutions become more accountable and whether confidence in government continues to grow.

At NIMC, we remain committed to strengthening Nigeria's national identity infrastructure and supporting the development of a trusted digital ecosystem that serves citizens, institutions and the broader national interest.

I call on ICAN, government institutions, regulators, technology providers and all relevant stakeholders to work together in building a digital governance framework that places integrity, accountability, transparency, security and inclusion at its core.

Let us use technology not merely to make government faster, but to make it fairer, more transparent and more accountable.

Let us build systems that do not simply record transactions, but help prevent irregularities.

Let us create institutions that do not merely collect information, but use it responsibly to make better decisions.

And let us ensure that Nigeria's digital transformation translates into tangible improvements in public service delivery, economic opportunity and national development.

The goal is clear: a Nigeria where technology strengthens trust, accountability drives performance, and transparency becomes a defining characteristic of governance.

Thank you for your attention.

God bless ICAN. God bless the Federal Republic of Nigeria.