LAUNCH OF CYBER AND INFORMATION SECURITY DIRECTIVE (CISD)

REMARKS

BY

DR. JOHNSON PANDIT ASIAMA
GOVERNOR, BANK OF GHANA

8TH FLOOR, URBAN BLOCK, BANK SQUARE

25 MARCH 2026

The Honourable Chief of Staff, Office of the President,
The Honourable Minister for Communications, Digital Technology, and Innovations,
The First Deputy Governor, Bank of Ghana,
Directors-General of Sister Regulatory Institutions (NPRA, NIC, SEC),
Chief Executive Officers and Managing Directors of Banks and Specialised Deposit-Taking Institutions,
Presidents of the Ghana Association of Banks and other Industry Associations,
Our Valued Partners from the Fintech Community,
Distinguished Ladies and Gentlemen.

Good morning.

It is my distinct honour and privilege to welcome you all to the official launch of the Bank of Ghana's revised **Cyber and Information Security Directive (CISD) 2026**.

The theme for this launch, **"A Safer and More Resilient Digital Financial Industry",** is not merely a slogan; it is the central pillar of our regulatory philosophy and a commitment we make to every Ghanaian who entrusts their accounts and transactions to this sector.

Today marks a significant milestone in our journey to protect Ghana's financial ecosystem. For years, our mandate has been clear: to ensure price stability and a sound financial system. However, in this digital age, that mandate has expanded. We are no longer just supervising capital adequacy ratios or liquidity positions; we are now, more than ever, safeguarding the **confidentiality, integrity, and availability** of the data that powers our economy.

THE EVOLVING LANDSCAPE

Over the last decade, innovations like Mobile Money, Cloud Computing, and Artificial Intelligence have revolutionised financial access and inclusion.

They have brought banking to the unbanked and sped up commerce in ways we could only dream of.

However, this progress has also invited sophisticated and persistent information security risks. From ransomware attacks that can paralyse a bank for days, to systemic data breaches that can shatter public trust in an instant, the threats we face are no longer just isolated IT incidents; they are **national security concerns**.

The Bank of Ghana recognised this shift years ago. The first Directive, issued in 2018, laid the groundwork. But we must be honest: a framework designed for the challenges of 2018 cannot

adequately solve the problems of 2026. The threat landscape has changed, and so must we. We have moved beyond simple compliance toward a posture of **active and collective cyber resilience.**

THE CYBERSECURITY ACT AND OUR MANDATE

This proactive stance is not just a matter of policy; it is a matter of law. As you are aware, the **Cybersecurity Act, 2020 (Act 1038)**, specifically Sections 41 to 48, designates the Bank of Ghana's Financial Industry Command Security Operations Centre (FICSOC) as the **Sectoral Computer Emergency Response Team (CERT)** for the entire financial industry.

This is a responsibility we do not take lightly. It mandates us to move beyond being a passive regulator and become an active defender and coordinator. It is in this spirit that we have developed this revised Directive, to give legal and operational impetus to our collective defence.

KEY PILLARS OF THE CISD 2026

The 2026 Directive is built on the pillars of robust governance, clear accountability, and proactive defence. It introduces several critical innovations designed to prepare us for the future:

1. **AI and Machine Learning Governance:** As financial institutions increasingly adopt AI for fraud detection, credit scoring, and customer service, we must ensure it is done with rigorous governance. This Directive provides the first comprehensive framework in the financial ecosystem to ensure these "black box" systems are fair, transparent, and secure.

2. **Cloud Computing Security:** We recognize that the risk-based, responsible, and secure adoption of cloud technology, specifically for the less critical aspects of our operations, is no longer optional; it is a business imperative. However, let me be clear: this Directive does not endorse the wholesale migration of core systems or sensitive data to the cloud. The Cybersecurity Act, 2020 (Act 1038) and the Data Protection Act, 2012 (Act 843) mandate data sovereignty.

   This means that the physical location of databases containing personal and financial information must remain within the territorial boundaries of Ghana. Only non-sensitive, front-end services may be hosted in the cloud, and even then, only through a risk-based, approved, and tightly controlled framework.

This Directive provides the clear rules of the road for such adoption, ensuring that as our institutions embrace the cloud in a compliant manner, their security posture migrates with them, and they remain fully aligned with all relevant laws and regulations.

3. **The Proportionality Framework:** We listened to the industry. We understand that a small rural bank does not have the same resources as a large multinational. This new framework scales our requirements based on an institution's size and risk profile, ensuring security is "fit-for-purpose" without being unduly burdensome.

4. **Board-Level Accountability:** Security is no longer just an IT problem; it is a strategic business risk. We now mandate that at least one member of your Board possesses verifiable expertise in cyber risk management. This ensures that security discussions happen at the highest level, right where strategic decisions are made.

5. **Inclusive Oversight:** A financial ecosystem is only as strong as its weakest link. I am pleased to announce that we are expanding the FICSOC's coverage. Beyond the universal banks, we are actively onboarding all Other Financial Institutions (Savings and Loans companies, Microfinance institutions), FinTechs, and our partner Regulators. We are building a unified shield for the entire sector.

SUSTAINING OUR COLLECTIVE DEFENCE

Distinguished ladies and gentlemen, building and maintaining a world-class defence capability like the FICSOC requires significant investment in infrastructure, advanced technology, and, most importantly, highly skilled personnel. As the Sectoral CERT, the Bank of Ghana has borne the initial cost of this critical national infrastructure to get it off the ground.

However, to ensure the **sustainability, continuous upgrade, and 24/7 operational effectiveness** of this shared service, we must move toward a model of shared responsibility. Just as we all contribute to the security of our physical communities, we must contribute to the security of our digital financial community.

Therefore, the Bank of Ghana is developing a sustainable **shared services model** for the FICSOC. We are committed to ensuring this model is transparent, fair, and provides clear value. It will ensure that the 'nerve centre' of our industry's cyber defence remains cutting-edge, well-staffed, and capable of protecting us all against the threats of tomorrow.

THE PATH FORWARD

Cybersecurity is not a destination; it is a continuous journey of vigilance and adaptation. As we look toward a future of Quantum Computing and Open Banking, our resilience will depend on three things: **Talent, Technology, and Trust.**

The Bank of Ghana remains your committed partner in this endeavour. This Directive is more than a set of rules to be complied with; it is a **collective pact** to protect the digital soul of our economy.

I urge all stakeholders here today to embrace these principles not just as a compliance exercise, but as a foundational pillar of your business strategy. Let us build a financial system that is not only prosperous but is also resilient, secure, and trusted by all Ghanaians.

Thank you for your unwavering commitment to this cause. I wish us all a successful and impactful implementation of the 2026 Directive.

God bless our homeland Ghana.