The Journal of Computer Science and Its Applications. An International Journal of the Nigeria Computer Society (NCS)
Vol.32, No.1, April, 2026

Governance and Regulatory Gaps in IoT Security Deployment in Nigeria: A Risk-Oriented Framework

Ogbu Nwani Henry*[1]
Department of Computer Science, Ebonyi State University, Ebonyi State, Nigeria.
ogbu.henry@ebsu.edu.ng

Ituma Chinagolum[2]
Department of Computer Science, Ebonyi State University, Ebonyi State, Nigeria
chinagolumituma@ebsu.edu.ng

Anyim Chukwuemeka[3]
Department of Computer Science, David Umahi Federal University of Health Sciences, Uburu, Ebonyi State.
anyimemy@gmail.com

Abstract
Recent advisories from the Nigerian Communications Commission Computer Security Incident Response Team (NCC-CSIRT) show that malware families such as Mirai, GRIDTIDE and COLDEYE target Internet of Things (IoT) devices and telecommunications infrastructures in Nigeria. These warnings are important because infected routers, cameras, and other connected devices can be converted into botnets for distributed DOS attacks, data theft and persistent intrusion. The problem is technical and reflects a wider governance weakness: security controls for IoT devices are known, but institutional arrangements needed to make those controls routine, enforceable and auditable remain uneven in many emerging economies. This paper examines governance and regulatory gaps in IoT security deployment through risk-oriented synthesis of official advisories, international standards and peer-reviewed literature. The analysis shows that global standards often assume enforcement capacity, skilled cybersecurity personnel, supply-chain visibility and sustainable funding. These assumptions do not always fit the institutional realities of emerging digital environments. The paper therefore proposes a four-stage IoT governance maturity framework: AdHoc Deployment, Policy-Aware Governance, Structured Governance, and Resilient Adaptive Governance. Each stage identifies indicators, transition requirements and risk-reduction outcomes. The framework provides policymakers, service providers and researchers with a practical roadmap for moving from reactive incident handling to proactive and adaptive IoT security governance.

Keywords: IoT Governance; Cybersecurity Policy; Regulatory Framework; Emerging Economies; Maturity Model; NCC-CSIRT.

1. INTRODUCTION

The Internet of Things has moved from a specialist technology into the everyday infrastructure of homes, campuses, hospitals, businesses and public services. Routers, cameras, sensors, smart meters, industrial controllers and health-monitoring devices now collect and exchange data continuously. These systems create efficiency and visibility, but they also widen the number of entry points available to attackers. In Nigeria, this risk has become more visible through NCC-CSIRT advisories reporting active malware campaigns against connected devices and telecommunications infrastructures [1], [2], [23].

The Mirai advisory is particularly instructive. Mirai does not depend on a complex mystery. It spreads because many IoT devices still run with default credentials, weak configurations or outdated firmware. Once compromised, devices can be grouped into botnets and used to launch large-scale distributed denial-of-service attacks against critical services [1],

[22]. GRIDTIDE and COLDEYE show a more sophisticated side of the same problem. GRIDTIDE hides command-and-control activity inside legitimate cloud services, while COLDEYE provides kernel-level persistence and deeper system control [2], [23]. Together, these threats show that IoT insecurity is no longer a distant possibility; it is already part of Nigeria's cyber-risk environment.

The issue, however, should not be framed only as a weakness in devices. Technical safeguards such as password replacement, firmware updates, secure boot, network segmentation, device certification and traffic monitoring are widely discussed in the literature and in standards [3], [15], [17], [20]. The deeper problem is that these safeguards are not always implemented consistently. Many organisations deploy devices before assessing risk, keep no reliable device inventory, lack skilled personnel for monitoring, and respond to incidents only after damage has occurred. Where governance is weak, even simple technical weaknesses can remain active for years.

IoT adoption in emerging economies therefore creates a policy dilemma. Governments want to encourage digital innovation, smart infrastructure, e-health, connected education and industrial automation. At the same time, regulatory institutions often lack the manpower, equipment, funding and legal coordination needed to supervise the security of thousands of imported and locally deployed devices. Nigeria illustrates this dilemma clearly. The country has several agencies with cybersecurity-related responsibilities, including the NCC, NITDA and the Office of the National Security Adviser, yet IoT security responsibilities remain dispersed across institutional boundaries. The result is a fragmented oversight environment in which advisories can be issued but follow-through may remain difficult.

This paper addresses that gap by examining IoT security governance as a risk-management problem rather than a purely technical problem. It reviews existing standards and advisories, analyses the risk landscape, and proposes a staged governance maturity framework that can guide emerging economies from ad hoc deployment toward resilient, adaptive oversight. The paper is organised as follows: Section 2 reviews relevant literature and standards; Section 3 explains the methodology; Section 4 discusses the risk landscape; Section 5 presents the proposed framework; Section 6 provides an implementation roadmap; Section 7 discusses implications; Section 8 states the limitations; and Section 9 concludes with future research directions.

2. LITERATURE REVIEW

2.1 International Standards and Their Assumptions

International bodies have developed several standards for information security, cybersecurity risk management and consumer IoT protection. The ISO/IEC 27001 standard requires organisations to establish an information security management system, assess risks and implement controls [14]. The NIST Cybersecurity Framework 2.0 organises cybersecurity practice around GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER, while also recognising that organisations mature from partial to adaptive practices [15]. The General Data Protection Regulation highlights privacy-by-design, data minimisation and breach-notification responsibilities that are highly relevant to data-intensive IoT systems [16]. ETSI EN 303 645 further provides baseline protections for consumer IoT, including unique passwords, secure updates, secure communication and resilience during network disruptions [17].

These standards are valuable because they provide a common language for security. They explain what good practice should look like and give organisations a benchmark for assessing risk. However, their usefulness depends on the institutional environment in which they are applied. Many standards assume that organisations have cybersecurity teams, audit routines, technical documentation, clear reporting structures and regulators that can inspect and sanction non-compliance. In many emerging economies, these assumptions are only partly present. A regulator may issue guidance, but lack the resources to verify thousands of deployments. A public agency may own connected devices, but have no specialist staff to maintain them. A service provider may understand the need for monitoring, but face budget and skills limitations.

2.2 National-Level Governance Challenges

The challenge of translating standards into enforceable practice is a recurring issue in IoT governance. Regulatory fragmentation is one of the most visible obstacles. IoT systems cut across telecommunications, data protection, national security, consumer protection, power, health, transport and local government. In Nigeria, the NCC regulates communications infrastructure and issues threat advisories, NITDA develops digital policy guidance, ONSA coordinates national cybersecurity strategy, while state governments and institutions deploy connected systems for their own operational needs.

Without a formal coordination mechanism, each institution may act within its own mandate while gaps remain between them.

Import dependence also weakens visibility. Many IoT devices used in emerging economies are manufactured outside the country. This makes it difficult to confirm how devices were designed, whether secure-update channels are available, and whether vendors will provide timely support when vulnerabilities emerge [13]. The NCC-CSIRT advisories refer to vulnerabilities in devices and systems that may not be locally manufactured [1], [2]. This means that national cybersecurity resilience depends not only on domestic policy but also on procurement standards, vendor accountability and supply-chain transparency.

2.3 The Nigerian Cyber Resilience Framework

The Cyber Resilience Framework for the Nigeria Communication Sector (CRF-NCS) represents a recent attempt to strengthen sectoral cybersecurity governance [19]. It sets out five pillars: Governance and Compliance, Risk Management, Cybersecurity Measures, Incident Management and Resilience, and Capacity Building and Awareness. It also introduces tiered compliance, requires service providers to appoint Chief Information Security Officers, encourages security operations centres, and gives timelines for incident detection and confirmation [19].

The CRF-NCS is important because it moves the conversation from general awareness to sector-specific duties. It recognises that resilience requires governance, reporting, monitoring, capacity building and collaboration. Yet, as a new framework, its practical effect will depend on implementation. Questions remain about enforcement capacity, reporting discipline, regulator-industry coordination, smaller service providers' compliance costs and the ability to extend lessons from the communications sector into other IoT-intensive sectors. These concerns make a staged maturity model useful, because it allows regulators to recognise where they currently stand and what must be built before full enforcement becomes realistic.

2.4 Synthesis and Research Gap

Existing literature on IoT security has often focused on device authentication, access control, encryption, edge-cloud architectures and intrusion detection [3], [20], [21]. These technical studies are necessary, but they do not fully explain why preventable weaknesses continue to recur. The recurring problem is that technical controls require governance systems to make them routine. Devices must be inventoried, procurement standards must be written, personnel must be trained, incidents must be reported, and regulators must be able to coordinate action. The research gap addressed here is the need for a governance maturity framework that takes institutional constraints seriously and provides a practical pathway for emerging economies.

Table 1: Governance Challenges and Implications

Finding	**Implication for framework design**
International standards often assume well-resourced institutions.	Frameworks should be adaptable to resource and capacity constraints.
Regulatory authority is spread across several agencies.	Coordination mechanisms are essential for consistent oversight.
Enforcement capacity remains limited.	Phased approaches with achievable milestones are needed.
Cybersecurity expertise is uneven across sectors.	Capacity building should be built into the framework, not added later.
Import dependence reduces supply-chain visibility.	Procurement rules and vendor verification should form part of governance.
User impact from cyber threats is already visible.	Governance failure should be treated as a public and economic risk.

3. RESEARCH METHODOLOGY

The study adopts a conceptual synthesis methodology. It draws on official Nigerian cybersecurity advisories, international standards, policy frameworks and peer-reviewed literature to develop a governance maturity model for IoT security in emerging economies. The method is appropriate because the goal is not to test a single technical control, but to organise existing evidence into a practical governance framework that can guide policy and institutional action.

Sources were identified from policy repositories and standards bodies, including NCC-CSIRT, NCC, NIST, ISO/IEC, ETSI and relevant academic databases. Search terms combined concepts such as "Internet of Things," "IoT governance," "cybersecurity regulation," "risk management," "emerging economies," "Nigeria," "critical infrastructure," and "maturity model." Sources were

included where they addressed IoT security, cybersecurity governance, regulatory coordination, standards, supply-chain risk or institutional constraints in digital security.

The analysis followed four steps. First, official advisories were reviewed to identify active threat patterns and local risk signals. Second, international standards were examined to identify expected governance capabilities. Third, the literature was used to group risks into technical, operational and strategic categories. Fourth, the maturity framework was developed by matching governance weaknesses to progressive institutional capabilities. The resulting model is therefore interpretive, but it is grounded in documented advisories, recognised standards and the emerging-economy governance literature.

4. RISK LANDSCAPE IN EMERGING IoT DEPLOYMENTS

4.1 Technical Risks

Technical risks are the most immediate and visible layer of IoT insecurity. Many connected devices still depend on weak default credentials, outdated firmware, insecure interfaces and poor configuration management. Mirai remains a useful example because its success depends on simple but widespread weaknesses. The NCC-CSIRT advisory confirms that Mirai-like threats remain active in Nigeria and can exploit devices that are poorly maintained or left with factory settings [1].

GRIDTIDE and COLDEYE show how the threat environment is also becoming more advanced. GRIDTIDE's use of legitimate cloud services as command-and-control channels makes detection harder, because malicious traffic can resemble ordinary cloud communication [2]. COLDEYE's kernel-level persistence is even more serious, since it can provide attackers with deep system access and long-term control [23]. These threats confirm that IoT risk now ranges from basic credential abuse to sophisticated intrusion.

4.2 Operational Risks

Operational risks emerge from the way devices are deployed, monitored and maintained. A technically secure device can become vulnerable when it is not patched, when no one knows it is connected, or when network traffic is never reviewed. Many organisations do not maintain complete inventories of their connected devices, and without an inventory, it is difficult to know which systems require updates or replacement. The NCC-CSIRT's recommendation that organisations monitor unusual outbound traffic implicitly recognises that operational monitoring is often weak [1].

Operational risk also includes weak incident reporting. If an organisation treats an infected device as an isolated technical problem, the wider ecosystem remains exposed. Incident information must move from affected users to service providers, regulators and response teams. The CRF-NCS addresses this by setting reporting timelines and encouraging service providers to build incident-management capacity [19]. The challenge is that these requirements must become daily practice rather than policy language.

4.3 Strategic Risks

Strategic risks appear when technical and operational weaknesses begin to affect national services, public confidence and economic activity. IoT systems increasingly support utilities, traffic management, telecommunications, healthcare, education and industrial processes. When such systems are compromised, the effect can extend beyond one device or one organisation. A botnet attack can disrupt public services; a poorly secured sensor network can expose sensitive information; a vulnerable industrial device can create safety and operational problems.

Import dependence deepens this strategic risk. If critical devices are sourced from vendors without adequate security assurance, the country may have limited ability to inspect firmware, demand timely updates or verify long-term support. This makes procurement standards and supply-chain security central to IoT governance. Figure 1 illustrates how device-level vulnerabilities can flow upward into operational failure, strategic exposure, national impact and human consequences.

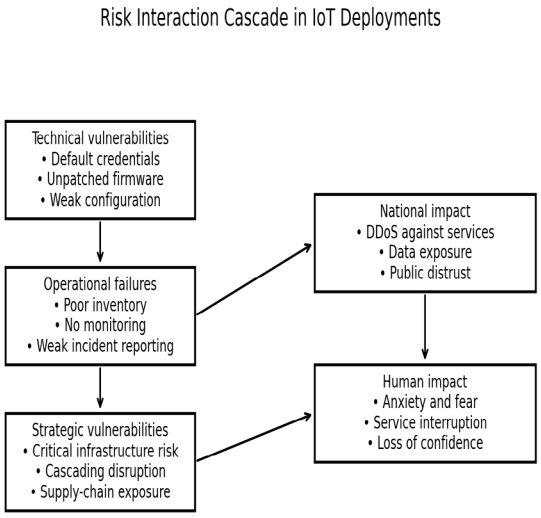


Figure 1: Risk interaction cascade in IoT deployments. The figure summarises how technical weaknesses can develop into operational, strategic and human impacts.

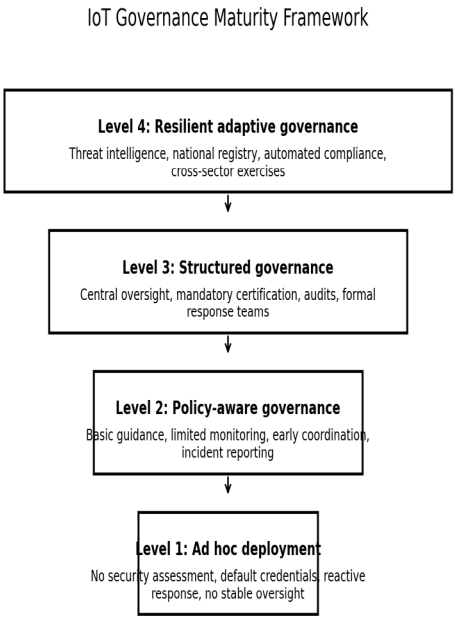


Figure 2: Four-stage IoT governance maturity framework. Each level builds institutional capacity before more advanced enforcement becomes practical.

5. PROPOSED IoT GOVERNANCE MATURITY FRAMEWORK

5.1 Overview

The proposed framework presents four stages of IoT security governance maturity: Ad Hoc Deployment, Policy-Aware Governance, Structured Governance, and Resilient Adaptive Governance. The model does not assume that every country or sector can immediately implement the most advanced requirements. Instead, it recognises that governance capacity grows through stages. Each stage builds on the previous one by adding awareness, coordination, enforcement, monitoring and adaptive response. This staged logic aligns with the maturity orientation of the NIST Cybersecurity Framework, which recognises that risk-management practices develop progressively [15].

5.2 Level 1: Ad Hoc Deployment Stage

The Ad Hoc Deployment Stage describes environments where devices are purchased and connected without formal security assessment. Policies are weak or absent, default credentials may remain unchanged, and incident response is reactive. Organisations may only become aware of a problem after malware activity has already affected services. The NCC-CSIRT advisories reflect this condition because they respond to active threats already spreading across the ecosystem [1], [2].

Typical indicators include absence of device inventories, no regular patching schedule, no formal monitoring, unclear responsibility for security, and limited awareness among end users. The main transition challenge at this stage is to build basic security culture. Practical early steps include awareness campaigns, minimum password rules, inventory creation, reporting channels and simple procurement guidance. These measures are inexpensive, but they create the foundation for stronger governance.

5.3 Level 2: Policy-Aware Governance Stage

At the Policy-Aware Governance Stage, institutions begin to recognise IoT security as a policy issue. Guidelines are issued, some organisations conduct basic assessments, and incident reporting becomes more visible. However, enforcement remains limited and compliance is often voluntary. Nigeria's policy environment reflects aspects of this stage, especially where guidance exists but implementation is uneven. The CRF-NCS shows movement toward stronger sectoral governance, but implementation capacity will determine its effect [19].

Progression from Level 2 to Level 3 requires moving from advice to accountability. Regulators need audit capacity, clear mandates and coordination structures. Organisations need staff who understand device security, risk registers and incident reporting. At this level, the most important question is no longer whether policies exist, but whether there is a credible mechanism for checking and improving compliance.

5.4 Level 3: Structured Governance Stage

The Structured Governance Stage introduces formal oversight. At this point, a lead authority or coordinated inter-agency arrangement is responsible for IoT security policy. Device certification becomes mandatory for critical sectors, procurement standards include security requirements, and compliance audits are conducted regularly. Advisories are backed by enforcement authority, and organisations that ignore known risks can be held accountable.

This stage also requires sector-specific working groups, operational incident response teams and formal reporting pipelines. The aim is to prevent weaknesses before they become incidents. For example, mandatory certification and procurement controls would reduce the number of devices that enter critical networks with default credentials or weak update mechanisms. Structured governance therefore turns security from a voluntary recommendation into an organisational duty.

5.5 Level 4: Resilient Adaptive Governance Stage

The Resilient Adaptive Governance Stage represents a mature and intelligence-driven system. At this level, national or sectoral registries provide visibility into critical IoT assets, threat intelligence is shared in real time, compliance monitoring is partly automated, and policies are updated as threats evolve. Cross-sector exercises are routine, and cooperation with international partners strengthens early warning and incident response.

At this stage, the governance system is not merely reacting to malware advisories; it is anticipating threats. Mirai-like scanning activity can be detected early, device owners can be notified quickly, and vulnerable systems can be isolated before they become part of a botnet. This level is difficult to achieve quickly, but it gives policymakers a long-term vision for national IoT resilience.

5.6 Transition Requirements

Table 2: Transition Requirements Between Governance Stages

Transition	Requirements	Local evidence or relevance
Level 1 to Level 2	Awareness programmes, basic guidelines, device inventory, incident reporting channels.	NCC-CSIRT advisories show that incident warning capacity exists, but wider awareness and basic controls are still needed [1].
Level 2 to Level 3	Central coordination, certification infrastructure, audit capacity, sector mandates and procurement standards.	Multiple agencies have relevant roles, while the CRF-NCS provides a sectoral framework that requires implementation support [19].
Level 3 to Level 4	Advanced threat intelligence, national registry, automated monitoring and international cooperation.	Expanded NCC-CSIRT capability and stronger threat-sharing platforms are needed for proactive defence [1], [19].

5.7 Risk Mitigation Across Stages

Table 3: Risk Mitigation Across Maturity Stages

Risk category	Level 1	Level 2	Level 3	Level 4
Technical risks	Mostly unaddressed; default credentials and unpatched devices persist.	Basic guidance is issued and some organisations act.	Mandatory standards and certification reduce insecure deployment.	Continuous monitoring and automated alerts improve early containment.
Operational risks	Reactive response; weak inventory and limited reporting.	Informal oversight and basic incident reporting emerge.	Formal procedures, audits and response teams become routine.	Automated compliance and mature response exercises are established.
Strategic risks	Largely unrecognised until disruption occurs.	Awareness grows through advisories and policy documents.	Coordinated response protects critical sectors.	Resilience is integrated into national planning and threat intelligence.

6. IMPLEMENTATION ROADMAP FOR EMERGING ECONOMIES

6.1 Budget Constraints and Resource Optimisation

Emerging economies often face tight public budgets, so IoT governance cannot depend on expensive national systems from the beginning. The first priority should be to protect high-impact sectors such as telecommunications, energy, transportation, healthcare and public administration. Early spending should focus on inventories, awareness, basic reporting, vulnerability scanning and procurement guidance. These are not glamorous interventions, but they reduce risk at relatively low cost. Over time, governments can seek development partnerships, regional cooperation and shared security services to support more advanced stages.

6.2 Capacity Building and Institutional Development

Capacity building is the heart of the roadmap. Regulations cannot work if the people expected to implement them lack the required skills. Regulators need cyber-risk analysts, auditors, incident responders and policy specialists. Public agencies need officers who can manage inventories, supervise vendors and report incidents. Industry needs trained staff who can run monitoring tools and interpret advisories. The CRF-NCS requirement for service providers to appoint CISOs and conduct training is therefore an important foundation [19].

Table 4: Capacity Building Timeline

Period	Focus	Target group	Suggested metric
Years 1-2	Awareness programmes, basic training, device inventory and password hygiene.	All relevant agencies and device-owning organisations.	Reduction in avoidable cyber incidents and increased incident reporting.
Years 3-4	Specialised regulator training, certification design and security operations capacity.	Lead regulators, service providers and critical infrastructure operators.	Establishment of audit units and certification procedures.
Years 5-7	Advanced threat intelligence, continuous professional development and sector exercises.	All mature stakeholders in critical sectors.	Proactive detection, coordinated exercises and routine threat sharing.

6.3 Public-Private Collaboration Framework

IoT security cannot be delivered by government alone. Regulators provide rules and oversight, but industry owns and operates much of the infrastructure. Academia contributes research, training and workforce development. Civil society can help with awareness and accountability. The NCC-CSIRT advisories demonstrate the value of public warning, while industry action is needed to implement the recommended controls [1]. The CRF-NCS proposal for threat intelligence sharing is therefore a useful step toward a more collaborative model [19].

Practical collaboration can begin with joint task forces linking NCC, NITDA, ONSA, sector regulators, service providers and academic experts. It can also include sector-specific working groups for telecommunications, power, health, finance and education. These groups should not exist only on paper; they should test reporting channels, share anonymised threat information, organise simulation exercises and publish lessons learned.

6.4 Phased Regulatory Enforcement

Enforcement should be phased because sudden full compliance may overwhelm organisations with limited capacity. Phase one should focus on voluntary guidelines, awareness campaigns and reporting. Phase two should introduce sector-specific mandates for critical infrastructure and government procurement. Phase three should add compliance audits, certification requirements and penalties for repeated non-compliance. Phase four should move toward adaptive enforcement using real-time risk data and automated compliance evidence. This sequence allows institutions to learn while still moving toward accountability.

6.5 Education and Workforce Development

Education is central to sustainable IoT governance. Universities and polytechnics should integrate IoT security, risk management, privacy and cyber-policy into computing, engineering and information systems programmes. Professional bodies should develop short certification pathways for regulators and practitioners. Public awareness campaigns should help users understand basic device security, including password changes, updates and safe configuration. The finding that many users have experienced negative cyber impacts indicates that end-user education is not optional [8].

6.6 Supply Chain Security Measures

Supply-chain security should become a formal part of public procurement. Government agencies and critical infrastructure operators should avoid purchasing devices without update support, documentation, unique credentials and basic certification. Vendors should provide security guarantees and, where appropriate, Software Bills of Materials for critical systems. Import screening, approved-vendor lists and local testing laboratories can help reduce the entry of high-risk devices into sensitive networks. These steps are especially important where countries depend heavily on imported IoT hardware.

Table 5: Implementation Roadmap Summary

Area	Level 1 to 2 actions	Level 2 to 3 actions	Level 3 to 4 actions
Budget	Prioritise critical sectors and low-cost awareness actions.	Seek international funding and shared service models.	Sustain national funding for monitoring and research.
Capacity	Train users and build basic reporting skills.	Develop specialist units and regulator certification.	Maintain advanced expertise and continuous development.
Collaboration	Create informal stakeholder engagement channels.	Set up joint task forces and sector working groups.	Operate real-time intelligence sharing platforms.
Regulation	Use voluntary guidelines and advisories.	Introduce sector mandates and procurement rules.	Move to full enforcement and adaptive policies.
Education	Run public awareness programmes.	Introduce university curricula and professional certifications.	Support executive education and applied research.

Supply chain	Publish basic procurement guidance.	Certify vendors and high-risk devices.	Implement import screening and local testing.

7. DISCUSSION

7.1 Synthesis of Key Findings

The analysis points to five connected findings. First, IoT security depends on governance foundations. Technical controls are useful only when institutions can require, monitor and verify their implementation. The NCC-CSIRT advisories show that basic controls such as changing default credentials and applying updates remain difficult to enforce at scale [1].

Second, emerging economies face challenges that cannot be solved by simply importing developed-country frameworks. Standards are still necessary, but they must be adapted to local realities such as scarce expertise, limited budgets, fragmented agencies and supply-chain dependence. Third, IoT risks cascade. Weak credentials or unpatched firmware can lead to operational failures, which can then become strategic risks for critical infrastructure. Fourth, governance maturity develops incrementally. A country cannot move from ad hoc deployment to adaptive governance without passing through awareness, coordination, enforcement and capacity-building stages. Fifth, the human consequences of weak governance are real. Cyber threats create anxiety, embarrassment, service disruption and distrust, especially where users feel powerless to protect their devices [8].

7.2 Implications for Policymakers

Policymakers should begin by assessing the current maturity level of each sector. Nigeria appears to be moving between Level 1 and Level 2 in many areas: advisories and frameworks exist, but preventive enforcement and coordinated oversight remain developing. The most useful early steps are practical and affordable: national awareness, device inventories, minimum security requirements, incident reporting templates and inter-agency coordination. Stronger enforcement should follow after institutions have built the capacity to implement and verify compliance.

7.3 Implications for Industry

Industry stakeholders should treat IoT security as a business and reputational issue, not merely a compliance burden. Service providers, vendors and organisations deploying IoT devices should expect regulation to become more demanding as threats increase. The recommended measures in NCC-CSIRT advisories—password changes, firmware updates, monitoring and segmentation—should be treated as routine security practice [1]. Firms that invest early in secure deployment will be better prepared for certification, audits and customer trust requirements.

7.4 Implications for Researchers

Researchers can strengthen the proposed framework by testing it empirically across sectors and countries. Case studies of telecommunications, universities, healthcare facilities and public utilities would help identify what enables or blocks movement from one maturity stage to another. More quantitative research is also needed to estimate infection rates, compliance costs, incident-reporting behaviour and the effectiveness of awareness programmes. The CRF-NCS provides a timely opportunity for longitudinal research on policy implementation [19].

7.5 Integration with Technical Security Frameworks

The framework is not intended to replace technical security architectures. Instead, it complements them. Standards such as NIST CSF and ETSI EN 303 645 explain what organisations should do, while the maturity model explains how emerging economies can build the institutional conditions needed to make those actions practical [15], [17]. Governance and technology must therefore be treated as mutually reinforcing. Without governance, technical recommendations remain optional; without technical standards, governance lacks operational detail.

8. LIMITATIONS

Table 6: Limitations of the Study

Category	Limitation
Conceptual nature	The framework is not yet empirically validated and stage definitions may require refinement through field studies.
Scope	The emerging-economy focus may not generalise to all national contexts or sectors.
Methodological approach	The study uses interpretive synthesis and qualitative risk

	categorisation rather than statistical testing.
Data limitations	Official advisories confirm threat presence but do not provide complete infection-rate data; institutional impact data remain limited.
Framework recency	The CRF-NCS is recent, so its implementation and effectiveness are yet to be fully evaluated.

These limitations should guide interpretation. The framework is best read as a structured policy tool and research agenda, not as a finished measurement instrument. Its value lies in helping stakeholders organise priorities and identify the institutional capabilities that must be built over time.

9. CONCLUSION AND FUTURE WORK

This paper has argued that IoT security in emerging economies cannot be secured by technology alone. The Nigerian experience, reflected in NCC-CSIRT advisories on Mirai, GRIDTIDE and COLDEYE, shows that known technical weaknesses continue to create serious risk when governance systems are weak [1], [2], [23]. Devices become dangerous not simply because they are connected, but because they are connected without inventory, monitoring, certification, maintenance and clear responsibility.

The paper contributes a risk-oriented view of IoT governance by linking technical vulnerabilities, operational weaknesses and strategic national risks. It also proposes a four-stage maturity framework that can guide policymakers from ad hoc deployment to resilient adaptive governance. The model emphasises awareness, coordination, enforcement, capacity building, supply-chain oversight and threat intelligence. It gives emerging economies a realistic pathway that recognises constraints while still pointing toward higher standards of resilience.

For policymakers, the priority is to move from reactive advisories to preventive governance. This means building coordination mechanisms, strengthening regulator capacity, aligning procurement with security requirements and supporting sector-level implementation. For industry, the priority is to adopt basic security measures before regulation forces compliance. For researchers, the priority is to validate the framework, measure maturity and study how governance reforms affect real-world incident rates. Future work should include multi-country case studies, sector-specific applications, cost-benefit analysis, maturity assessment tools and longitudinal evaluation of the CRF-NCS. The security of IoT systems will depend not only on smarter devices, but on stronger institutions capable of governing them.

REFERENCES

[1] NCC-CSIRT, “Mirai Malware Threat Active in Nigeria Cyberspace,” Nigerian Communications Commission Computer Security Incident Response Team, Advisory ID: NCC-CSIRT-2025-001, 2026.

[2] NCC-CSIRT, “GRIDTIDE Backdoor and UNC2814 Cyber Espionage Campaign Targeting Telecommunications Infrastructure,” Nigerian Communications Commission Computer Security Incident Response Team, Advisory ID: NCC-CSIRT-2026-012, 2026.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

[4] H. Lee, S. Lee, and T. Kim, “Smart grid and IoT: A comprehensive survey,” IEEE Access, vol. 8, pp. 123456–123478, 2020.

[5] J. Lee, B. Bagheri, and H. A. Kao, “A cyber–physical systems architecture for Industry 4.0-based manufacturing systems,” Manufacturing Letters, vol. 3, pp. 18–23, 2015.

[6] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, “The Internet of Things for health care: A comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.

[7] E. Oyo-Ita et al., “Identification of students in higher institutions in Nigeria using IoT-based attendance system,” 2024.

[8] D. Samson, D. I. Vincent, D. T. Apere, and Tonubari, “Investigating the impact of cyberspace threats on electronic device users in Nigerian tertiary institutions (a case study of IJBCOE, Sagbama),” International Journal of Scientific and Research Publications, vol. 13, no. 6, pp. 135–140, 2023.

[9] M. Weiss and D. Werth, “Cross-border policy harmonization challenges for IoT governance,” Policy & Internet, vol. 15, no. 4, pp. 799–820, 2023.

[10] A. Geyer and R. Broglio, “IoT governance and institutional capacities in developing economies,” Journal of Information Policy, vol. 14, pp. 243–269, 2024.

[11] R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, fog computing and the Internet of Things: A survey,” Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.

[12] P. Voigt and A. Von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham, Switzerland: Springer, 2017.
[13] R. Nair, H. Bedi, and S. Sahu, "Supply chain risks in IoT hardware: Governance implications," International Journal of Critical Infrastructure Protection, vol. 38, p. 100516, 2023.
[14] ISO/IEC, "ISO/IEC 27001: Information security management systems—Requirements," International Organization for Standardization, Geneva, Switzerland, 2022.
[15] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper (CSWP) NIST CSWP 29, Gaithersburg, MD, USA, Feb. 2024.
[16] European Parliament and Council, "Regulation (EU) 2016/679 (General Data Protection Regulation)," Official Journal of the European Union, vol. L119, pp. 1–88, 2016.
[17] ETSI, "ETSI EN 303 645: Cyber Security for Consumer Internet of Things," European Telecommunications Standards Institute, Sophia Antipolis, France, 2020.
[18] M. Z. Chowdhury, R. Hasan, M. R. Islam, and M. Z. Rahman, "IoT security challenges in developing countries: A governance perspective," Technology in Society, vol. 71, p. 102112, 2023.
[19] Nigerian Communications Commission, "Cyber Resilience Framework for the Nigeria Communication Sector (CRF-NCS)," Version 1.0, Feb. 2026.
[20] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access control for IoT: A survey of existing research, dynamic policies and future directions," Sensors, vol. 23, no. 4, p. 1805, 2023.
[21] A. Tripathi and V. Varadharajan, "Security frameworks for hybrid cloud–edge IoT architectures," Computers & Security, vol. 124, p. 102929, 2023.
[22] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.
[23] NCC-CSIRT, "COLDEYE Kernel-Level Malware Targeting Telecom Networks," Nigerian Communications Commission Computer Security Incident Response Team, Advisory ID: NCC-CSIRT-2026-013, 2026.