ADVOCAAT
LAW PRACTICE

CLIENT ALERT:

The Nigerian Communications Commission's Guidance Note on the Implementation of the Cyber Resilience Framework for the Nigerian Communications Sector (CRF-NCS)

LAGOS | ABUJA | CALABAR

INTRODUCTION

The Nigerian Communications Commission ("NCC" or "the Commission") has issued a Guidance Note on the Implementation of the Cyber Resilience Framework for the Nigerian Communications Sector ("CRF-NCS" or "the Framework")[1]. The Guidance Note supplements the CRF-NCS issued by the Commission on 23 February 2026.

The Guidance Note operationalises the CRF-NCS by setting out how licensed communications service providers are expected to implement the Framework in practice. It identifies the specific cybersecurity controls applicable to service providers, classifies providers into the relevant tiers, prescribes the applicable maturity levels for the controls, and specifies the evidence required to demonstrate compliance. The key provisions are highlighted below.

TIERED AND MATURITY-BASED APPLICATION

A central feature of the Guidance Note is that obligations are not applied uniformly. What this means is that service providers are classified into three tiers:

a. Tier 1, comprising core networks, spectrum holders, and all communications service providers;

b. Tier 2, comprising providers with national coverage, shared infrastructure, and aggregate or emerging technology providers; and

c. Tier 3, comprising support service providers to other communications service providers[2].

Each control is also tagged by maturity level (Baseline, Intermediate, or Full), indicating the standard a provider is expected to meet at the applicable stage of implementation, rather than a single fixed compliance bar.[3] Interestingly, some controls are pitched differently by tier. A good example is the mandatory cybersecurity budget allocation, which is tagged as a full maturity control for Tier 1 and Tier 2 providers, but as a Baseline control for Tier 3 support service providers, meaning the obligation applies to Tier 3 providers immediately rather than as a later-stage target.[4]

MANDATORY CYBERSECURITY BUDGET ALLOCATION

The Guidance Note requires service providers to allocate an adequate percentage of their total company budget to cybersecurity. The Board of Directors and senior management[5] will oversee this dedicated budget, and service providers must also ensure that their budget, staff, and resources support their cybersecurity risk strategy. They must have a process for monitoring cybersecurity spending and adjusting future budgets to support resilience. Compliance with this provision is demonstrated by providing an approved document showing the budget allocated to cybersecurity.

GOVERNANCE, THE DESIGNATED OFFICER, AND BOARD OVERSIGHT

Service providers must appoint a senior official, known as the Designated Officer (or Chief Information Security Officer/CISO for Tier 1 and Tier 2 providers), to manage cybersecurity risks, respond to

[1] Guidance Note: Implementation of Cyber Resilience Framework for the Nigerian Communication Sector (CRF-NCS), July 2026.
[2] *Ibid*., p. 2–14.
[3] *Ibid*., p. 2.
[4] *Ibid*., GC-BS.S1–S4 (Tier 1&2, tagged [F]) with the corresponding Tier 3 budget and spending control (tagged [B]).
[5] *Ibid*., GC-BS.S1–S4.

incidents, and oversee the implementation of the Board-approved cybersecurity policy.[6] The NCC must be notified in writing of the appointment, and the acknowledgement must be kept for audit purposes. Service Providers designated as owners of Critical National Information Infrastructure (CNII) must ensure that the Designated Officer's roles and responsibilities comply with the 2024 CNII Order. The Board, Partners, or Proprietor must also establish a Cybersecurity Committee that meets at least twice a year to review the implementation of the cybersecurity policy and report its findings to the Board for necessary action.

INCIDENT REPORTING TIMELINES

The Guidance Note requires service providers to report cybersecurity incidents within specific timelines. Any cyber-attack, cybersecurity incident, or breach affecting a provider's systems, network, or critical assets must be reported to NCC-CSIRT within four hours of detection or awareness. Full details of the incident must then be submitted through the NCC-CSIRT Incident Reporting Portal within 24 hours. Service Providers must also submit quarterly reports covering cyber-attacks, threats, incidents, and mitigation measures from the previous quarter within 15 days after the quarter ends. Providers designated as CNII owners must also follow the required CNII incident escalation procedures. Sensitive information shared between providers must be classified using the Traffic Light Protocol (white, green, amber, or red).

RECOVERY OBJECTIVES AND DATA LOCALISATION

Where a disruption affects one or more critical systems, providers must classify it as a "Disaster" within 30 minutes of the incident. This classification should be based on the business impact analysis and comply with the NCC Disaster Recovery Guidelines 2023. Providers should aim to restore critical operations within two hours (the Recovery Time Objective, or RTO) and limit data loss to no more than 15 minutes[7] (the Recovery Point Objective, or RPO).

Separately, providers must keep call logs, user IDs, and traffic data in-country for at least two years. Law enforcement may access this information only when they present a valid warrant.[8]

INTERFACE WITH THE NIGERIA DATA PROTECTION ACT

The Guidance Note brings data protection requirements directly into the cybersecurity compliance framework, rather than treating them separately. Service providers must appoint a Data Protection Officer registered with the Nigeria Data Protection Commission (NDPC), report personal data breaches to both the NDPC and the NCC in accordance with the NDPA, conduct Data Protection Impact Assessments (DPIAs) for high-risk activities such as biometric data collection and AI-driven analytics, and maintain detailed Records of Processing Activities (RoPA) that are subject to annual audits.[9]

This means that organisations seeking Data Controllers and Processors of Major Importance (DCPMI) registration under the NDPA's General Application and Implementation Directive will need to meet overlapping data protection and cybersecurity compliance requirements.

[6] *Ibid.*, GC-RRA.S3–S5 (Tier 1&2); CM-CH.S5 (Tier 3).
[7] *Ibid.*, CIRMR-IReP.S2(1).
[8] *Ibid.*, GC-LR.S1.
[9] *Ibid.*, CM-DP.S4(5)–(9); GC-LR.S2–S4.

COMPLIANCE TIMELINE AND EVIDENTIARY ARTEFACTS

Each control in the Guidance Note is linked to specific evidence that a provider must be able to produce when requested. Examples include an approved IT asset inventory, an incident response plan, a supply chain risk management strategy, and valid ISO 27001 or equivalent certifications, depending on the specific control.[10]

As under the original Framework, providers are still expected to achieve full compliance within 12 months of the Framework's issuance. The July Guidance Note does not appear to restart this deadline. Instead, it provides much more detail on the specific measures and evidence providers will need to have in place before the deadline.

IMPLICATIONS FOR STAKEHOLDERS

Licensed communications service providers should first confirm their Tier classification, as this determines which controls apply to them and the maturity level at which they will initially be assessed.

Tier 1 and Tier 2 providers should prioritise setting aside a dedicated cybersecurity budget that is visible to the Board, appointing and formally notifying the NCC of a Designated Officer or CISO, and ensuring that their incident response procedures can meet the required reporting timelines. These include notifying the NCC-CSIRT within four hours, submitting the required information through the portal within 24 hours, and completing the quarterly reporting cycle within 15 days.

Tier 3 support service providers should be aware that some controls, including cybersecurity budget allocation, apply to them at the Baseline level rather than being future requirements.

Providers that hold or process personal data should also ensure that their NDPA compliance measures, including DPO registration and DPIA procedures, are consistent with the cybersecurity requirements in the Guidance Note. The two regulatory frameworks are intended to operate together rather than as separate compliance obligations.

Finally, entities designated as CNII owners under the 2024 Gazette should ensure that their escalation procedures are formally documented, regularly tested, and ready to be activated when required.

CONCLUSION

The July 2026 Guidance Note makes the CRF-NCS more detailed and easier to audit. It sets different requirements based on a provider's tier and maturity level, introduces clear reporting deadlines, and specifies the evidence providers must maintain to demonstrate compliance. For communications sector operators, the immediate priority should be to assess their current practices against the controls that apply to their tier, address any gaps at the Baseline level, and develop a clear plan to reach Intermediate and Full maturity before the compliance deadline.

Our Technology and Data Protection practice group monitors developments in Nigeria's cybersecurity and digital infrastructure regulatory landscape. For further inquiries or clarification on how the Guidance Note may affect your operations, please contact our team.

CONTACTS

ROTIMI AKAPO
rotimi.akapo@advocaat-law.com

ADEYEMI OWOADE
adeyemi.owoade@advocaat-law.com

INIMFON EKPENYONG
inimfon.ekpenyong@advocaat-law.com

FAVOUR ODUNOWO
favour.odunowo@advocaat-law.com

AYOOLUWA ADEKOJE
ayooluwa.adekoje@advocaat-law.com

LAGOS OFFICE
13 Norman Williams Street
Off Keffi Street, Ikoyi
Lagos Nigeria

ABUJA OFFICE
Nigerian National Merit Award House Enspire
1st Floor Room 3
Plot 22 Aguiyi Ironsi Way Maitama Abuja
Nigeria

CALABAR
Akom Building
15 Murtala Mohammed Highway Calabar
Cross River
Nigeria

TELEPHONE: (LOS)+234 02014547932 (ABJ)+234 8105340496

EMAIL: info@advocaat-law.com **WEBSITE:** www.advocaat-law.com