CYBER RESILIENCE FRAMEWORK FOR NIGERIA COMMUNICATION SECTOR (CRF-NCS)

DATE: February 2026

VERSION 1.0

TABLE OF CONTENTS

LIST OF TABLES

List of Figures

Note to Readers on How to Use this Framework and its Annexures

This document includes annexures that provide supporting documents to complement the main framework. These annexures outline the baseline expectations, standards, and sample templates for service providers to aid in the implementation of the framework. To use it effectively:

- Framework Pillars – These are the five broad areas of the framework.
- Standards – They expand the pillars into specific standards, requirements, and best practices.
- Use of Codes – Each standard has a unique code derived as follows:
  - GC-LR.S1 = Governance & Compliance Pillar – Legal & Regulatory Domain, Standard 1)
- Annexures – Provides a breakdown to guide the uniform implementation of the standards relative to the tier of the service provider.

The table below shows the pillars and their corresponding codes:

PILLAR	CODE RANGE
Governance & Compliance	GC-LR.S1 – GC-C.S4
Cyber Risk Management	CRM-AR.S1 – CRM-RA.S8
Cybersecurity Measures	CM-DP.S1 – CM-MR.S6
Incident Management & Resilience	CIRMR-IRP.S1 – CIRMR-RM.S9
Capacity Building & Awareness	CBA-CSD.S1 – CBA-CECC.S3

The annexures are not meant to replace organisational policies or regulatory directives; rather, they serve as additional information and templates to promote consistency and uniform implementation of the framework.

Readers are encouraged to consult the annexures and use the outlined information to aid in understanding and applying the framework.

1.0 EXECUTIVE SUMMARY

The growing dependence on digital infrastructure has made the communications sector a critical enabler for economic resilience, national security, and citizen well-being. As cyber threats become more sophisticated, persistent, and transnational, the need for sector-specific approaches to cybersecurity has become more urgent, especially for high-value sub-sectors like the communications sector, given their role in enabling critical infrastructure.

A comprehensive cybersecurity risk management framework, developed by the Nigerian Communications Commission (NCC), aims to foster a unified and resilient cybersecurity stance while strengthening the protection of telecom infrastructure against cyberattacks. Furthermore, protecting consumer data, privacy, and trust while ensuring alignment with national cybersecurity strategies and international best practices is an additional objective of the framework.

The Cyber Resilience Framework for the Nigerian Communication Sector (CRF-NCS) is primarily built on two approaches: **cybersecurity and cyber resilience**. It emphasises cyber resilience because the communications sector is recognised as a critical subsector in Nigeria's National Cybersecurity Policy and Strategy. The CRF-NCS is a process-focused, standards-based framework built around **Five Core Pillars** of cyber resilience: **Governance & Compliance**, **Risk Management**, **Cybersecurity Measures, Incident Response, Management & Resilience,** and **Capacity Building & Awareness**. These pillars support sector-specific cybersecurity goals and serve as the foundation for a comprehensive set of standards and guidelines, ensuring uniform implementation.

Each service provider is expected to develop a cybersecurity and cyber resilience framework, establish internal cybersecurity governance structures, and appoint a cybersecurity role with responsibility and authority. Service Providers are also expected to conduct regular risk assessments, submit compliance reports, and participate in joint sectoral threat intelligence initiatives by sharing threat intelligence with the **NCC-CSIRT,** serving as the sectoral SOC. Finally, the framework emphasises cybersecurity capacity building and awareness for the Board of Directors, staff, and the customers of service providers.

The framework underscores the importance of addressing emerging security domains, such as Artificial Intelligence and Machine Learning, Quantum Secure Cryptography, Cloud Computing, and the cybersecurity implications of Virtualised Networks.

CRF-NCS comprises incident management protocols that are designed to be risk-informed, tier-sensitive, and resilience-focused. A robust tiered compliance monitoring and audit mechanism is also included, detailing the responsibilities of the regulator and service providers. The implementation roadmap adopts a phased and risk-tiered approach specifying compliance obligations by tier across 12 months. The success of the framework will be tracked through a set of Key Performance Indicators (KPIs) to monitor sectoral cybersecurity capabilities over time. To simplify and streamline the compliance reporting process, the CRF-NCS provides standardised formats for reports and submissions in the annexures.

2.0 INTRODUCTION

2.1 Background and Context

The global escalation of cyber threats has elevated cybersecurity to a critical national priority, with the communications sector increasingly targeted due to its pivotal role in enabling internet access, data transmission, digital identity services, and national emergency response systems. As Nigeria's communications landscape continues to expand rapidly, this growth is accompanied by heightened exposure to cyber risks, increased sophistication of attacks, and rapid evolution of the threat landscape.

The Nigerian Communications Commission (NCC) is the government institution responsible for fostering a competitive, safe, and efficient communications environment in Nigeria. The NCC, by mandate, is collaborating with industry stakeholders to secure Nigeria's digital ecosystem and ensure that both service providers and consumers benefit from a safe and resilient cyberspace.

NCC employs a multifaceted approach to address the evolving challenges of cybersecurity in Nigeria. This approach encompasses not only reactive measures, but also proactive strategies aimed at anticipating and mitigating emerging threats. One proactive strategy is the development of a cybersecurity framework to guide governance and operations of cybersecurity across the communications ecosystem. Accordingly, the NCC has developed a comprehensive cybersecurity framework for the Nigerian Communications Industry.

The framework aims to strengthen Nigeria's cybersecurity posture by ensuring compliance with regulatory standards and enhancing national security through improved threat detection, response, and risk mitigation strategies. Furthermore, the cybersecurity framework will enhance the resilience of telecom service providers, service providers, and critical network infrastructure providers against evolving cyber threats, leading to increased customer satisfaction and national security.

2.2 Objectives

The objectives of this framework include:

i. Promoting a unified, consistent, and resilient cybersecurity posture across the communications industry.
ii. Enhancing the protection of communications infrastructure and services from cyberattacks.
iii. Safeguarding consumer data, privacy, and trust in digital services.
iv. Ensuring alignment and implementation of the Nigerian Communications Act (2003), National Cybersecurity Policy and Strategy (NCPS) 2021, the Nigeria Data Protection Act, 2023, the Official gazette on the designation and protection of Critical National Information Infrastructure (CNII) Executive Order, 2024, and international best practices.
v. Ensuring sector-wide capacity to anticipate, detect, respond to, and recover from cyber threats.

2.3 Scope and Applicability

The scope of the framework encompasses responsibilities of service providers towards cybersecurity governance, risk management, implementation of cybersecurity measures, cybersecurity incident management, and the need for comprehensive cybersecurity capacity building and awareness. The framework is applicable and enforceable on all communication service providers who provide services as defined in the NCA (2003). (see Annexure IX for the list of licensed categories).

3.0 GOVERNANCE AND INSTITUTIONAL ARRANGEMENTS

3.1 Overview

Effective cyber risk governance requires well-defined institutional roles, a collaborative approach, and clear lines of accountability. This section outlines the proposed governance model for implementing and sustaining the objectives of the cybersecurity framework.

3.2 Key Governance Bodies and Their Roles

i. **Nigerian Communications Commission (NCC):** The Commission will serve as the lead sector regulator, responsible for implementing and enforcing this framework. NCC maintains a sectorial CERT known as NCC-CSIRT for coordinating cybersecurity incidents in the Communications sector.

ii. **ngCERT:** The National CERT (ngCERT) operates as the national technical coordination centre for cyber incident response, intelligence dissemination, and stakeholder capacity building. The ngCERT will serve as the final coordinating CERT for managing cybersecurity incidents in Nigeria

iii. **National Cybersecurity Coordination Centre (NCCC):** This is the government agency responsible for providing national-level oversight through the implementation of the National Cybersecurity Policy and Strategy (NCPS) and ensuring coordination across sectors and government tiers.

iv. **Nigeria Data Protection Commission (NDPC):** This public entity was established under the Nigeria Data Protection Act 2023, and is responsible for safeguarding data privacy, enforcement of regulations, and promoting responsible data handling in Nigeria.

v. **Other relevant government agencies responsible for cybersecurity activities in Nigeria.**

3.3 Coordination Mechanisms

To encourage collaborative partnership and strengthen national resilience coordination, the framework proposes the establishment of the following governance and coordination structures:

i. **NCC Cybersecurity Steering Committee (N3CSC):** This committee shall carry out the oversight responsibilities on this framework regarding implementation, compliance, ongoing review, etc. It shall

be charged with the responsibility for matters relating to cybersecurity in the communications sector.

ii. **Communication Sector Information Sharing and Analysis Centre (CS-ISAC)**: A platform for threat intelligence information sharing and analysis with relevant stakeholders like peer service providers, vendors, academia, and national as well as international authorities (NCCC, NPF-CCC, NFI-CERT, NITDA-CERRT, DSS, etc.)

3.4 Service Providers' Obligations

The following obligations and responsibilities are entrusted to each communication service provider.

i. **Cybersecurity and Cyber Resilience Framework**: Develop a cybersecurity and cyber resilience framework or strategy for their organisation with the following minimum components:
   - Establishing internal cybersecurity governance structures
   - Appointing a cybersecurity officer or focal point.
   - Conducting regular risk assessments and submitting compliance reports.
   - Participating in joint sectoral threat intelligence initiatives and sharing threat intelligence with NC-CSIRT.
   - Conduct mandatory cybersecurity capacity building and awareness sessions for the board, staff, and customers.

ii. **Compliance Responsibility**: Ensure compliance with the relevant provisions of this framework.

iii. **Mandatory Reporting**: Service providers must report cyber incidents within the designated timelines outlined in this framework.

iv. **Performance Audits**: Service provider and NCC will conduct periodic audits and assessments to ensure compliance with this framework.

v. **Public Reporting**: Participate in the annual sectoral cybersecurity research and reporting process. Such reports will be published to enhance transparency and public awareness of cybersecurity among sector stakeholders.

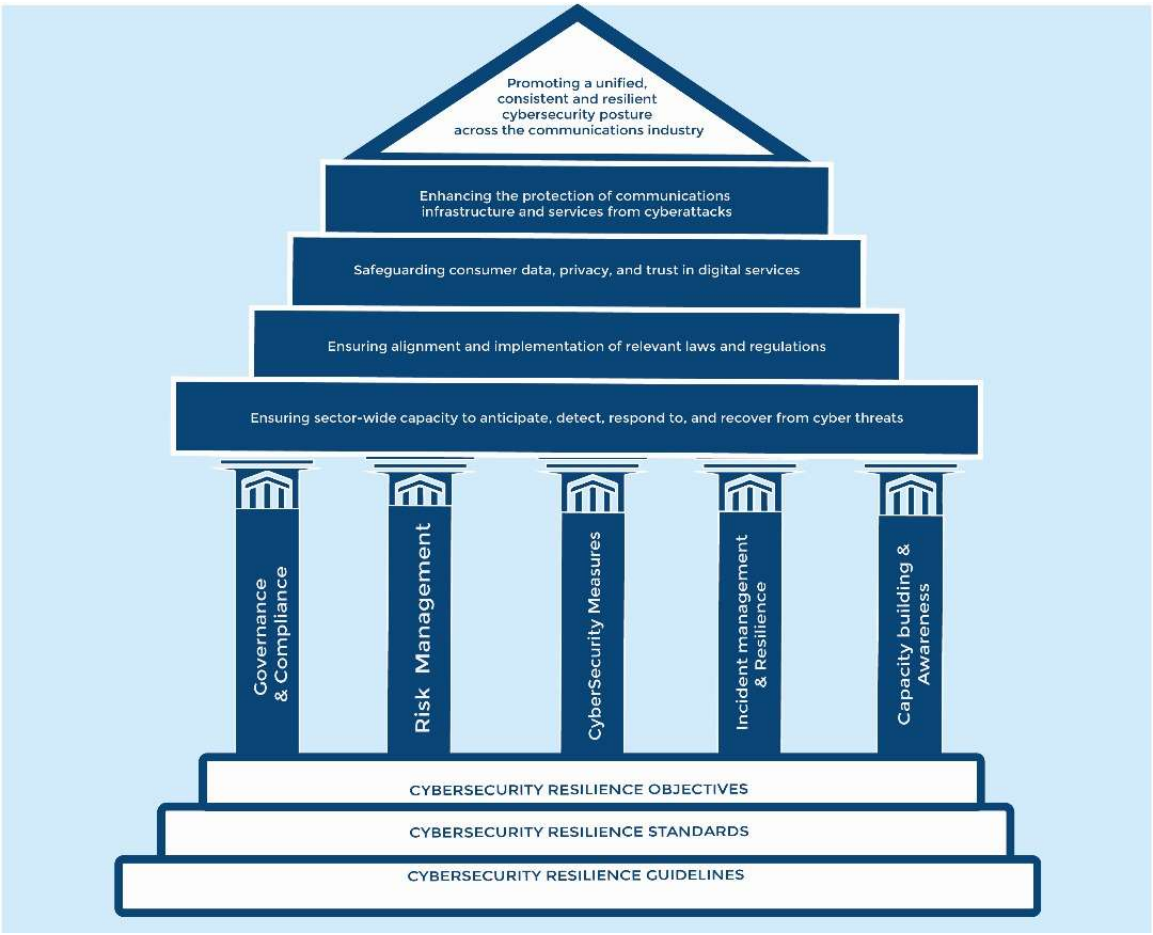
4.0 FRAMEWORK STRUCTURE AND MODEL

4.1 Overview

The CRF-NCS is a process-focused, standards-based framework built around five core pillars of cyber resilience.

i. **Governance & Compliance (GC):** This pillar ensures service providers implement governance policies, designate cybersecurity leadership, and comply with regulations and national laws.
ii. **Risk Management:** The pillar covers asset management, threat analysis, situational awareness, and information sharing.
iii. **Cybersecurity Posture:** This pillar addresses technical and organisational protective measures that secure digital assets. This includes data protection, access controls, network security, cyber hygiene, and third-party risk management.
iv. **Incident Response, Management & Resilience:** This pillar ensures the sector is prepared to detect, respond to, and recover from cyber incidents. Key components include incident response planning, monitoring systems, and recovery mechanisms.
v. **Capacity Building & Awareness:** This pillar covers cybersecurity capacity building, skill acquisition, cybersecurity awareness, talent development, research, and collaborative engagements among stakeholders.

4.2 CRF-NCS Framework



4.3 Approach to CRF-NCS

The Cyber Resilience Framework for the Nigerian Communication Sector (CRF-NCS) was developed with a special focus on incorporating resilience into the entire IT and OT environments of service providers. Service Providers in the communication sector either own or manage critical national information infrastructure, making them targets of cyberattacks from both state and non-state actors. Consequently, the cybersecurity standards developed within this framework are derived from the backdrop of this national responsibility to safeguard the well-being of Nigerians.

In addition, the framework emphasises the importance of governance and supply chain risk management in protecting service providers' assets. It also addresses emerging security domains such as Artificial Intelligence and Machine Learning, Quantum Secure Cryptography, Cloud Computing, and Virtualised Networks. Additionally, it focuses on data classification

and localisation, API security, secure coding practices, as well as the implications of adopting a Zero Trust Architecture in securing networks.

Furthermore, CRF-NCS outlines a variety of cybersecurity measures, including the categorisation of systems and critical assets, personnel training, incident response and planning, recovery strategies for critical cyber assets, vulnerability assessments, and more. More deliberately, one of its pillars is dedicated to cybersecurity capacity building and awareness to help address Nigeria's specific cybersecurity skill gap. CRF-NCS includes provisions covering areas such as cybersecurity requirements for third-party service providers, Software as a Service (SaaS) solution, hosted services, data classification, and audits of software solutions, applications, and products used by service providers.

CRF-NCS requires all service providers to establish effective security monitoring mechanisms through a Security Operations Centre (SOC). This SOC can be operated internally by the service providers or their group, a virtual SOC (vSOC), or a third-party managed SOC. The goal is to enable continuous monitoring of security events and facilitate the timely detection of any abnormal or malicious activities.

Recognising that some service providers may find compliance with cybersecurity guidelines challenging due to limited knowledge, expertise, and the costs associated with establishing their own SOC, CRF-NCS mandates that NCC-CSIRT should effectively perform the Sectoral SOC (S-SOC) responsibilities. The aim is to provide tailored cybersecurity support and solutions to these service providers, helping them meet security requirements more effectively. Additionally, a Cyber Capability Index (CCI) will help service providers monitor and assess their cybersecurity and cyber resilience journey on a periodic basis. To simplify and streamline the compliance reporting process, the CRF-NCS provides standardised formats and templates for reports and submissions.

4.4 The Structure of CRF-NCS

The framework is primarily built on two concepts: cybersecurity and cyber resilience. It emphasises cyber resilience because the communications sector is recognised as a critical sub-sector in the National Cybersecurity Policy and Strategy. Additionally, several infrastructure components within the telecom sector have been officially designated as Critical National

Information Infrastructure (CNII) in the Official Gazette through the "Designation and Protection of Critical National Information Infrastructure Order, 2024." This order identifies specific ICT systems across various sectors as CNII to ensure their protection and safeguarding.

The framework's structure encompasses both proactive and reactive measures. Proactive measures encompass various aspects, including governance, risk management, cybersecurity awareness, and numerous cybersecurity measures to protect service providers' IT and OT assets. Cyber resilience (reactive) measures include the ability to detect, respond to, and recover from cybersecurity incidents. The framework also specifies guidelines to ensure that standards are implemented uniformly.

The summary of the CRF-NCS is as follows:

i. **Cyber Resilience Function: PROACTIVE | Cybersecurity Process: GOVERNANCE** *(GC-LR.S1 ↔ GC-RM.S5)*
    a. Service Providers shall be responsible and accountable for compliance with all relevant legal and regulatory frameworks as applicable in Nigeria
    b. The service providers shall demonstrate a thorough understanding of the sector's cybersecurity challenges, objectives, and priorities to effectively guide their actions and decision-making.
    c. Service Providers shall define, communicate, and enforce cybersecurity roles, responsibilities, and authorities to promote accountability, facilitate performance evaluation, and support ongoing improvement.
    d. Service Providers shall document and implement a set of approved cybersecurity and cyber resilience policies and procedures to formalize their cybersecurity efforts.
    e. Service Providers shall establish a cyber risk management framework to identify, assess, mitigate, and monitor risks, supported by clearly defined cybersecurity processes and procedures
    f. Service Providers shall utilise organisation-wide cybersecurity risk management activities, performance, and outcomes to inform, improve, and refine the risk management strategy.

g. The service providers shall be accountable for establishing processes to identify, assess, and mitigate supply chain risks through effective third-party risk management.
h. The service Providers' cybersecurity budget is strategically allocated to align with specific cybersecurity objectives and their associated implementation activities.

ii. Cyber Resilience Function: PROACTIVE | Cybersecurity Process: COMPLIANCE *(GC-C.S1 ↔ GC-C.S4)*

a. Service Providers shall ensure compliance with all relevant laws, regulations, circulars, etc., issued by NCC and NCCC. Accordingly, service providers shall be responsible and accountable for any violations of the same.
b. Service Providers shall put in place appropriate systems and procedures to ensure compliance with the provisions (i.e., applicable standards and guidelines) of the CRF-NCS.

iii. Cyber Resilience Function: PROACTIVE | Cybersecurity Process: IDENTIFY, PRIORITIZE, AND MANAGE RISKS *(CRM-AR.S1 ↔ CRM-RA.S8)*

a. The leadership of service providers shall approve the list of critical systems based on their sensitivity and criticality for business operations, services, and data management.
b. The service providers shall develop or adopt a resilience-based risk management approach that strengthens the service providers' ability to absorb shocks, recover quickly, and adapt to evolving threats.
c. The service providers' cyber risk management strategy/framework shall include regular assessments (including post-quantum risks) of the likelihood and impact of adverse events or attacks, along with defined measures to mitigate identified risks.

iv. Cyber Resilience Function: PROACTIVE | Cybersecurity Process: SECURE *(CM-DP.S1 ↔ CM-MR.S6)*

a. Service providers shall implement technical and organizational measures to safeguard data (at rest, in transit, and in use), ensuring confidentiality, integrity, and availability of data.

These measures may include encryption, data loss prevention, regular backups, and logical or physical separation of data sources.

b. Development and testing environments must be separated from the production environment for critical software or application development.

c. Service providers shall implement measures for managing the digital identities, accounts, credentials, and authentication mechanisms for on-premises and cloud resources based on the principle of least privilege and segregation of duties.

d. Service providers shall define and implement technical security requirements across all network layers, including Core, Transmission/IP, Access, and Management, for all deployed generations of communication technologies (e.g., 2G, 3G, etc.), ensuring end-to-end encryption, authentication, and integrity checks for network traffic.

e. Service providers shall implement a Zero-Trust Architecture (ZTA) that secures micro-perimeters across the entire network and provides the ability to identify, protect, detect, respond, and recover from evolving attacks.

f. Service providers shall ensure that cybersecurity audits and VAPT are conducted to detect vulnerabilities in the IT and OT environments of critical systems.

g. Service providers shall implement measures to ensure that endpoint devices, networks, APIs, removable media, laptops, mobiles, etc., are secured with proper authentication and authorisation mechanisms.

h. Relevant industry cybersecurity standards and frameworks shall be mandatory for service providers as they provide relevant security standards.

v. Cyber Resilience Function: PROACTIVE | Cybersecurity Process: DISCOVER *(CIRMR-IRP.S1 ↔ CIRMR-DP.S3)*

a. Service providers shall establish or contract a Cyber Security Operations Centre (SOC) to monitor the network, endpoints, physical environment, personnel, malicious code, third-party activities, and detect unauthorised access, devices, and software.

b. Service providers shall measure the functional efficacy of their own SOC on a biannual basis in accordance with the relevant guidelines.

c. Service providers shall conduct security assessments of live systems by simulating attacker actions (red teaming) to evaluate the effectiveness of cybersecurity measures, processes, and personnel, and update the security plan as necessary.

vi. Cyber Resilience Function: REACTIVE | Cybersecurity Process: RESPOND *(CIRMR-CCMP.S1 ↔ CIRMR-CCMP.S11)*

a. Service providers shall develop and implement a comprehensive Cyber Crisis Management Plan (CCMP) that includes scenario-based Standard Operating Procedures (SOP).

b. Service providers shall conduct thorough investigations of cybersecurity incidents, including forensic analysis when necessary, to identify root causes, understand threat actor behaviour, trace lateral movements, and implement measures to prevent recurrence.

c. Service providers shall mandatorily get onboarded to the NCC-CSIRT's Vulnerability and Threat Exposure Management (VTEM) platform and other ngCERT initiatives as notified from time to time.

d. Service providers shall mandatorily report cybersecurity breaches and incidents to NCC-CSIRT, in line with the provisions of this framework.

vii. Cyber Resilience Function: REACTIVE | Cybersecurity Process: RECOVER *(CIRMR-IRP.S1 ↔ CIRMR-IRP.S6)*

a. Service providers shall comply with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO), specified in their Business Continuity Plan (BCP) document, while executing recovery plans for the restoration of critical systems and services after a cybersecurity incident.

b. Service providers shall conduct drills at least annually to test various recovery scenarios.

c. Service providers shall communicate recovery activities to internal and external stakeholders as well as executive and management teams.

viii. Cyber Resilience Function: REACTIVE | Cybersecurity Process: RESILIENCE *(CIRMR-RM.S1 ↔ CIRMR-RM.S9)*

a. Service providers shall proactively adjust cybersecurity measures and controls to address vulnerabilities and anticipate emerging or future threats.
b. Service providers shall periodically exercise a service-specific documented Business Continuity Management (BCM) process.
c. Service providers' cyber resilience capabilities shall be monitored through periodic drills (at least annually) to ensure safe and timely restoration of critical operations.

ix. Cyber Resilience Function: PROACTIVE & REACTIVE | Cybersecurity Process: EMPOWER *(CCB-CSD.S1 ↔ CCB-CECC.S3)*

a. Service providers shall regularly conduct role-based cybersecurity capacity building to ensure necessary stakeholders (e.g., third-party) have the necessary skills, and regularly update training programmes to reflect new threats, technologies, and industry trends.
b. Service providers shall ensure senior executives and Board members understand their cybersecurity responsibilities, and mandate dedicated training on cybersecurity, cyber resilience, and system hygiene.
c. Service providers are encouraged to promote and incentivise cybersecurity research, development, and innovation in Nigeria's tertiary institutions.
d. Service providers shall support and adhere to relevant governance frameworks and partnership initiatives to ensure the resilience of critical infrastructure through government collaboration with public and private service providers.

4.5 Future proofing of CRF-NCS

It is anticipated that emerging security trends will influence cybersecurity investments in the communications sector. Recognising these emerging contexts is crucial, as it allows for informed decision-making regarding current security initiatives, with a comprehensive understanding of the long-term environment. This knowledge also helps ensure that new security measures are as effective and impactful as possible.

Quantum computing could become a reality in the near future, with the potential to compromise many of the encryption schemes currently in widespread use. As a result, quantum computing might emerge as one of the most significant cybersecurity threats, potentially exposing communication systems to cyberattacks. Although the timeline for large-

scale adoption of quantum technology remains uncertain, its potential as a cyber threat to the communication ecosystem is already a cause for concern. The CRF-NCS includes provisions to tackle 'harvest now – decrypt later' attacks through ongoing risk assessments and the implementation of robust data protection measures.

The evolution of communication technologies will introduce new security considerations, including advancements in IoT device authentication and identification, as well as an expanded attack surface. Notable developments such as (e)SIM and (e)UICC technologies, coupled with enhanced Extensible Authentication Protocol (EAP) security features, will enable more sophisticated authentication mechanisms, broader identity management, and the expanded addressing capacity offered by IPv6. At the same time, the growing use of virtualisation and reliance on cloud infrastructure, particularly public clouds, will require fresh security models as mobile networks increasingly align with traditional IT environments. Of particular importance, network slicing will create distinct, purpose-built virtual network segments. Each slice will demand tailored, domain-specific security policies to protect sensitive operations and data. Maintaining consistent and robust protection across these slices and their interfaces will be crucial to preventing vulnerabilities and avoiding points of compromise.

The framework will be regularly updated to reflect the evolving maturity of technologies and their adoption by service providers, ensuring it effectively addresses the future cybersecurity requirements of the communications sector.

5.0 RESILIENCE-BASED RISK MANAGEMENT APPROACH

5.1 Purpose of the Risk Management Approach

In today's digitally dependent environment, cyber risks are no longer just IT issues; they are existential business and national security concerns. The communications sector is an enabler of digital services, emergency communications, and many critical national infrastructures rely on the sector for effective functioning. Consequently, resilience must be embedded at the heart of the sector's operations, which can best be achieved through a resilience-focused risk management process

The resilience-based risk management approach will integrate traditional risk mitigation, enhancing the service providers' capacity to absorb shocks, recover rapidly, and adapt to evolving threats. Instead of aiming solely to avoid failure, this approach prioritises preparedness, continuity, and agility in the face of uncertainty. Furthermore, the approach ensures that service providers can sustain critical operations, respond effectively to disruptions, and recover rapidly, regardless of the evolving threat landscape.

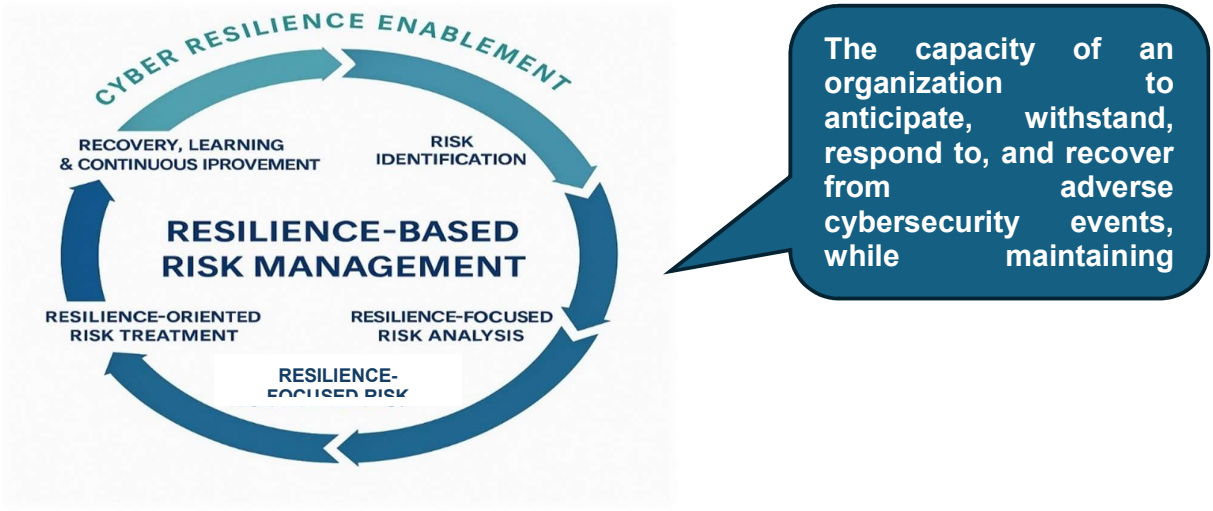


Figure 5.1.1: Resilience-Based Risk Management Model

This model integrates **cyber resilience thinking** throughout the process - from governance to risk management, implementation of cybersecurity measures, and incident management.

5.2 Sectoral Risk Tiers and Applicability

CRF-NCS follows a tiering approach and classifies the service providers based on a set of criteria as described below:

i. **Tier 1:** Service providers who own, lease, and/or operate core networks, have leased spectrum resources, and all entities providing any form of communications service in Nigeria.
ii. **Tier 2:** Service providers with national coverage, aggregate service, provide shared infrastructure, and other emerging technology service providers.
iii. **Tier 3:** All other service providers who provide support services to other communication service providers.

A full list of service providers' tiers by license category is provided in Annexure II.

6.0 CYBER RESILIENCE CAPABILITY FRAMEWORK

The framework offers a systematic approach to implementing diverse solutions for cybersecurity and cyber resiliency. To enhance understanding and simplify compliance, the document is organised into five (5) parts:

i. **Part I: Objectives and Standards**: – This part contains framework objectives and standards, etc.
ii. **Part II: Resilience-based Risk Management Approach:** The overall essence of the CRF-NCS is to build resilience in the operations of service providers. Resilience enables service providers to quickly recover from such attacks and return to Business As Usual (BAU) within the RTO and RPO specified by the Service Providers.
iii. **Part III: Compliance Formats:** This part outlines compliance responsibilities, audit report timelines, and standard formats for submitting CRF-NCS compliance reports, among other relevant details.
iv. **Part IV**: **Implementation Plan**: This part provides a comprehensive roadmap for implementing the framework, detailing specific actions, deadlines, and responsibilities for regulators, service providers, and other key stakeholders.
v. **Part V:** Various annexures like standards, compliance/reporting formats, and templates to serve as a guide to perform certain cybersecurity functions or guide uniform reporting to NCC.

6.1 CYBERSECURITY RESILIENCE FRAMEWORK – OBJECTIVES AND STANDARDS

The framework has established a set of cybersecurity standards encompassing the five (5) pillars. These standards are obligations on the service providers to achieve cyber resilience in their operations and critical services. The standards are outlined in Annexure XI.

Annexure XIV presents the CRF-NCS, illustrating how its pillars contribute to achieving the sector's goals, while the accompanying standards guide service providers in enhancing cyber resilience across the communications industry. A set of guidelines will be released as part of the implementation documents to ensure that standards are implemented uniformly.

7.0 INCIDENT MANAGEMENT AND REPORTING PROTOCOLS

Incident management is a critical element of the cybersecurity framework, central to maintaining operational continuity, minimising impact, and enhancing sectoral resilience. In alignment with Pillar 4 - Cybersecurity Incident Response, Management, and Resilience, the framework adopts a coordinated and standardised incident management and reporting structure. This approach enables service providers to effectively respond to, recover from, and learn from cybersecurity events, while reinforcing sector-wide situational awareness and preparedness. This section outlines the processes, procedures, and responsibilities for incident detection, classification, response, escalation, and post-incident evaluation. The protocols (as described in the standards and guidelines) are designed to be risk-informed, tier-sensitive, and resilience-focused.

7.1 Sectoral Incident Lifecycle

The framework defines a six-phase incident lifecycle, ensuring consistency across all service provider categories:

S/N	PHASE	KEY ACTIONS
1	Preparation	Develop incident response plans, assign roles, train personnel, and deploy monitoring and alerting systems.
2	Detection & Reporting	Identify suspicious activity, verify events, and initiate reporting through structured channels.
3	Classification & Triage	Assess scope and severity using the sectoral risk classification matrix; activate response teams.
4	Containment	Isolate affected systems or services, and prevent further spread or exploitation.
5	Eradication & Recovery	Remove threat vectors, restore systems, validate integrity, and resume operations.
6	Post-Incident Review	Conduct after-action assessments, document lessons learned, and update response plans and resilience measures.

Table 7.1.1: CRF-NCS Incident Lifecycle

7.2 Incident Severity Classification & Notification

The framework will adopt a two-step reporting approach as follows:

i. Reporting timeline for detection - 4 Hours
ii. The confirmation reporting timeline - 24 hours, with periodic 4-hour updates after the first detection.

Service providers are required to classify and report incidents with potential impact based on the following matrix:

LEVEL	DEFINITION	Reporting Window to NCC-CSIRT
Critical	National impact, data breach involving sensitive personal information, system-wide outage	See Annexure IV
High	Service disruption to multiple users, attempted large-scale attack	See Annexure IV
Medium	Targeted attacks, malware infections, and misconfigurations with risk exposure.	See Annexure IV
Low	Isolated or non-impacting security observations.	See Annexure IV

Table 7.2.1: CRF-NCS Incident Severity Classification

Service providers must maintain a dedicated focal point for incident reporting, with clearly defined escalation and contact protocols in place.

8.0 MONITORING, AUDITING, AND COMPLIANCE

8.1 Monitoring Responsibilities

To ensure the cybersecurity framework is implemented consistently and effectively across the sector, NCC, being the sector regulator, shall oversee ongoing compliance and performance monitoring. This will be supported by:

i. Self-assessment tools shall be provided to service providers.

ii. Regulatory reporting dashboards for real-time visibility using a Governance, Risk, and Compliance (GRC) management platform

iii. Performance scorecards that are aligned with the pillars of the framework.

8.2 Audit Responsibilities

Service providers will be subject to **internal and external audits** to ensure compliance with the framework's provisions. Audit obligations shall vary by tier as defined in Table 8.2.1.

TIER	Auditing Body	Periodicity
TIER 1	NCC or approved third-party auditors	Annually
TIER 2	NCC or approved third-party auditors	Annually
TIER 3	Self-assessment and self-audit using standard tools prescribed by NCC	Biannual

Table 8.2.1: CRF-NCS Audit Responsibilities

8.3 Tiered Compliance Responsibilities

Recognising the diversity within the communications sector, the framework adopts a **tiered compliance approach** based on the classification described above.

Each tier is associated with a corresponding set of graduated cybersecurity obligations, reporting, and audit requirements, scaled according to factors

such as geographic operational coverage, risk exposure, user base, and the impact of their services on the sector's overall functionality.

8.4 Compliance Period

Compliance with this framework will take effect on February 23, 2027, which is 12 months after the date of issuance. The commission retains the power to start a compliance review and demand earlier compliance than what is outlined in section 10.0 of this framework, as long as the implementation is in line with that provision.

Service providers shall establish appropriate systems and procedures to ensure compliance with the provisions (including applicable standards) of CRF-NCS. Additionally, they must conduct cybersecurity audits in accordance with CRF-NCS requirements after the commencement date. The cyber audit reports, along with any other required documentation, shall be submitted at least annually or as required by NCC. Service providers shall submit compliance reports to NCC-CSIRT using the process and forms detailed in this framework.

8.5 Evaluation Metrics and Indicators

A set of Key Performance Indicators (KPI) has been developed to monitor and evaluate the impact of the framework on the sector (See Appendix X)

8.6 Enforcement and Corrective Measures

Non-compliance will be enforced in line with the expectations and provisions of the Enforcement Processes Regulations 2019, as may be amended from time to time.

8.7 Sector-Wide Transparency and Benchmarking

To promote accountability, NCC will publish:

i. Annual cyber risk compliance reports (aggregated, anonymized)

ii. Sectoral benchmarking data

iii. Framework improvement recommendations based on audit findings.

9.0 CAPACITY BUILDING, AWARENESS, AND CYBERSECURITY CULTURE

Effective cybersecurity in the communications sector depends not only on technological controls but also on the human and institutional capacity to implement, adapt, and sustain cybersecurity practices. Recognising the sector's diverse levels of cybersecurity maturity, the framework identifies capacity building and awareness as a strategic pillar for long-term resilience.

This section outlines the sectoral strategies for developing and promoting cybersecurity awareness, embedding the culture of cyber hygiene, and institutionalising a **security-first mindset** across all stakeholders.

9.1 Strategic Objectives

The capacity building and awareness agenda under this framework aims to:

i. Enhance the **technical and operational capabilities** of service providers to prevent, detect, and respond to cyber threats.
ii. Promote a **culture of cybersecurity responsibility** at all organisational levels.
iii. Institutionalise **continuous learning and knowledge sharing** within and across sector stakeholders.
iv. Address the **skills gap and workforce shortage** in cybersecurity through targeted development programs.
v. Foster **collaboration among public, private, and academic stakeholders** for talent development and innovation.

9.2 Key Cybersecurity Training Responsibilities

S/N	SCOPE	DESCRIPTION
1	Service Providers Workforce Training	Service providers should implement structured cybersecurity training programs for relevant teams.
2	Executive Awareness	Boards and leadership of service providers should undergo cybersecurity awareness and governance training.
3	Consumer Awareness Campaigns	Service providers should conduct public campaigns to promote digital

		safety, scam recognition, and responsible technology use.
4	Technical Skills Development	Service providers should conduct national certification programs and partnerships with academia to deepen technical expertise in areas such as SOC operations, threat intelligence, and penetration testing.
5	Simulation and Tabletop Exercises	NCC shall facilitate annual drills to test incident response and crisis coordination.

Table 9.2.1: Capacity Building Key Focus Areas

10.0 IMPLEMENTATION

The successful adoption of the Cybersecurity Framework across the Nigerian communications industry will be guided by a structured, inclusive, and adaptive implementation strategy. The implementation roadmap outlined in this section provides a clear, time-bound, and risk-oriented approach to guide the operationalisation of the framework across all service provider tiers.

The roadmap emphasises a phased rollout, capacity and resource considerations, and regulatory responsibilities to ensure the successful implementation of the framework.

10.1 Implementation Timelines and Compliance Obligations

	COMPLIANCE OBLIGATION	PERIOD	TIER	SCOPE
1	Baseline cybersecurity requirements (by Tier)	6 months	All tiers	Compliance with baseline requirements
2	Intermediate cybersecurity requirements (by Tier)	9 months	All tiers	Compliance with mandatory standards
3	Full cybersecurity requirements (by Tier)	12 months	All tiers	Compliance with all standards

Table 10.1.1: CRF-NCS Implementation Roadmap

"All Communications Service Providers across all tiers shall achieve full compliance within twelve (12) months from the effective date of the official release of this Framework (February 23, 2026). Notwithstanding the foregoing, the Commission reserves the right to initiate compliance reviews and require earlier compliance where circumstances so warrant, subject to reasonable notice."

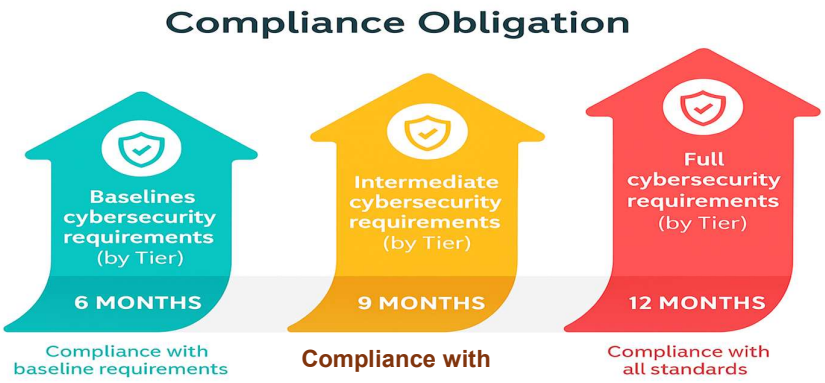


Figure 10.1.1: CRF-NCS Implementation/compliance obligation

11.0 REVIEW AND UPDATE MECHANISM

To maintain continued relevance, effectiveness, and alignment of the Framework with emerging threats, evolving technologies, and regulatory priorities, a structured review and update mechanism has been established.

This mechanism ensures that the framework is a living document, sensitive to evolving threat landscape, emerging cybersecurity contexts, alignment with national cybersecurity priorities, and international best practices.

11.1 Documentation and Change Management

Every revision shall be accompanied by:

i. A **Change Log,** summarizing what has been updated and why.

ii. An **Update Bulletin,** issued to all stakeholders via NCC channels of communication.

iii. A versioning system indicating major vs. minor updates.

iv. Retention of archived versions for transparency and traceability.

ANNEXURES

	ANNEXURE NUMBERING	DESCRIPTION
1	**Annexure (I)**	Template for breach notifications to NCC
2	**Annexure (II)**	List of service provider tiers
3	**Annexure (III)**	Defines the scope for Vulnerability Assessment and Penetration Testing (VAPT)
4	**Annexure (IV)**	Standard Operating Procedure (SOP) for incident reporting to NCC-CSIRT
5	**Annexure (V)**	Security controls for customer-facing applications
6	**Annexure (VI)**	Encryption guidelines for data at rest
7	**Annexure (VII)**	Security measures for data transmission over the internet
8	**Annexure (VIII)**	Encryption standards for data in cloud environments
9	**Annexure (IX)**	List of licensed categories
10	**Annexure (X)**	Key Performance Indicators
11	**Annexure (XI)**	CRF-NCS Standards
12	**Annexure (XII)**	Sample cyber attack scenario template
13	**Annexure (XIII)**	Baseline security requirements
14	**Annexure (XIV)**	CRFNCS framework structure

GLOSSARY

Term / Acronym	Meaning
CRF-NCS	Cyber Resilience Framework for the Nigeria Communication Sector
Service Provider	
NCC - Nigerian Communications Commission	The national regulatory authority for the communications industry in Nigeria.
NCC-CSIRT	Nigerian Communications Commission Computer Security and Incident Response Team
ngCERT - Nigeria Computer Emergency Response Team	National body responsible for cybersecurity incident coordination and advisory.
NITDA - National Information Technology Development Agency	Provides policy guidance and regulation for IT development in Nigeria.
NDPA	A data protection law enforced by NDPC.
NDPA	Nigeria Data Protection Commission
ONSA	Office of the National Security Adviser
Resilience-Based Risk Management	A cybersecurity approach that prioritizes preparedness, adaptation, response, and recovery from cyber incidents.
Tier1/Tier 2/Tier3 Service Providers	Classification of communications service providers based on risk exposure, infrastructure complexity, and market size.
Incident Management	Structured processes to detect, respond to, contain, and recover from cybersecurity incidents.
CSIRT - Computer Security Incident Response Team	A group responsible for managing and responding to cyber threats.
SIEM - Security Information and Event Management	Technology that provides real-time analysis of security alerts.

Threat Intelligence	Information about cyber threats and threat actors that helps prevent or mitigate cyber-attacks.
Control Catalogue	A set of cybersecurity controls organised into domains for implementation by sector service providers.
NIS	Network and Information Systems
ISO/IEC 27001	International standard for Information Security Management Systems (ISMS).
ISO/IEC 27035	An international standard providing guidelines for cybersecurity incident management.
NIST CSF - National Institute of Standards and Technology Cybersecurity Framework	A U.S.-based framework for managing cybersecurity risks.
Risk Register	A documented repository of identified cyber risks, their impact, and mitigation strategies.
Baseline Controls	Minimum cybersecurity requirements mandated for service providers based on their tier classification.
MFA - Multi-Factor Authentication	An access security method requiring two or more verification factors.
KPIs - Key Performance Indicators	Metrics used to assess cybersecurity performance and implementation progress.
SOP - Standard Operating Procedure	Documented step-by-step instructions to achieve consistency in operations.
RTO - Recovery Time Objective /RPO - Recovery Point Objective	Business continuity metrics defining recovery targets.
ZTA - Zero Trust Architecture	A security model that assumes no user or system is trusted by default, even if inside the network perimeter.
Audit Trail	A chronological record of cybersecurity-related actions and events for accountability and analysis.

Phishing	A type of cyber-attack that uses fraudulent messages to trick users into revealing sensitive information.
Cyber Hygiene	Routine practices and procedures that maintain and improve cybersecurity health and posture.
Attack Surface	The total exposure points (devices, systems, endpoints) that can be exploited in a cyber-attack.
Security Posture	The overall cybersecurity strength and readiness of an organisation based on its controls and capabilities.
Mitigation Measures	Actions taken to reduce the severity or impact of cyber risks.
Playbook	A documented set of incident response procedures to be followed in specific cybersecurity scenarios.
MNOs	Mobile Network Service Providers
ISPs	Internet Service Providers
VAS	Value Added Services
NCPS	National Cybersecurity Policy and Strategy
Licensee	An organization with official permission to operate within the sector
GC	Governance and Compliance
Service Providers	An organization carrying out business within the communications industry (in the framework context)
SOC	Security Operation Centre
vSOC	Virtual-Security Operation Centre
S-SOC	Sectorial-Security Operation Centre
CCI	Cyber Capability Index
CNII	Critical National Information Infrastructure
NCCC	National Cybersecurity Coordination Centre
Critical Systems	A system that, if it fails, may pose a risk to the operation of a service provider
on-premises	Hosting a service on one's hardware – either renting space in the data centre or locally in one's premises.

Cloud	A distributed collection of servers that host software and infrastructure, and it is accessed over the Internet.
Least Privilege	An information security concept in which a user is given the minimum levels of access or permissions needed to perform his/her job functions.
IPv4/IPv6	A protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks
2G/3G/4G/5G - Second/Third/Fourth/Fifth Generation	Generations of mobile communications technologies.
E2EE – (End-to-End Encryption)	A method of implementing a secure communication system where only communicating users can participate.
AA - Authentication/Authorisation	Vital information security processes that administrators use to protect systems and information.
Network Traffic	The amount of data moving across a network at a given point in time.
VAPT - Vulnerability Assessments, and Penetration Testing	A process to help organizations identify and fix security weaknesses before attackers can exploit them.
vulnerabilities	A weakness in an IT system that can be exploited by an attacker to deliver a successful attack.
APIs - Application Programming Interface	A set of programming code that allows two programs to talk to each other.
Removable Media	A type of storage device that can be removed from a computer whilst the system is running
CCMP - Cyber Crisis Management Plan	A comprehensive plan that outlines the procedures, roles, and responsibilities required to effectively respond to a cyber crisis.
VTEM - Vulnerability and Threat Exposure Management	A platform for managing potential threats and vulnerabilities to corporate assets
BCM - Business Continuity Management	A holistic management process that oversees and implements strategies to address the risk of unexpected distruptions.

DRP - Disaster Recovery Plan	A written plan for protecting critical applications in the event of a major hardware or software failure or destruction of facilities.
(e)SIM	An industry-standard digital SIM eliminating the need for a physical SIM card
(e)UICC - Embedded Universal Integrated Circuit Card	A component of a Subscriber Identity Module (SIM) card enabling switching of Mobile Network Service Providers (MNOs)
EAP - Extensible Authentication Protocol	An authentication framework that allows for the use of different authentication methods for secure network access technologies
Telecom Backbone	A robust, high-speed network that links multiple local networks into a single wide-area network
Data leakage	The process of sensitive information being unintentionally exposed to unauthorised parties.
Malware - malicious software	An intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems
CISO - Chief Information Security Officer	A senior-level executive who oversees an organisation's information and cybersecurity.
SDLC - Secure Software Development Life Cycle	A cost-effective and time-efficient process that development teams use to design and build high-quality software.
BAU - Business as Usual	A normal activity of a business that are necessary to maintain its operations.
ACLs - Access Control List	A set of rules that either allow access to a computer environment or deny it.
VLANs - Virtual Local Area Network	a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.
IDPS - Intrusion Detection and Prevention Systems	A network monitoring strategy that supports threat detection by passively monitoring traffic and actively blocking suspicious or malicious behavior once it is flagged.
IDS/IPS - Intrusion Detection/Intrusion Prevention System	Part of a network security measure taken to detect and stop potential incidents.

SDH - Synchronous Digital Hierarchy	A multiplex technology used in telecommunications. SDH allows data streams with low bit rates to be combined into high-rate data streams.
SONET - Synchronous Optical Network	A standard for connecting fiber-optic transmission systems sold in North America only
OSPF - Open Shortest Path First	A link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm.
BGP - Border Gateway Protocol	A set of rules that determine the best network routes for data transmission on the internet.
SSH - Secure Socket Shell	A cryptographic network communication protocol that enables two computers to securely communicate
SNMPv3 - Simple Network Management Protocol version 3	A network monitoring protocol focusing on encrypting and authenticating data packets over the network.
RAN - Radio Access Network	A major component of a wireless telecommunications system that connects individual devices to other parts of a network through a radio link.
BTS - Base Transceiver Stations	A piece of equipment that facilitates wireless communication between user equipment (UE) and a network
SSL/TLS - Secure Sockets Layer/Transport Layer Security	An encryption protocol that is used to encrypt and protect data sent over the internet or a computer network.
SaaS - Software as a Service	A cloud computing service model in which a provider delivers application software to clients while managing the required physical and software resources.
NFI-CERT – Nigeria Financial Industry Cybersecurity Emergency Response Centre	Sectoral Cybersecurity Emergency Response Centre for the Financial Sector in Nigeria.
CBN – Central Bank of Nigeria	The Central Bank of Nigeria (CBN) is the central bank and apex monetary authority of Nigeria, established by the CBN Act of 1958
PQC - Post-Quantum Cryptography	Quantum-resistant encryption that can withstand powerful quantum computers

ZTA - Zero Trust Architecture	A security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.
IAM - Identity and Access Management	A framework of policies, processes, and technologies that enable organisations to manage digital identities and control user access to critical corporate information
PKIX - Public Key Infrastructure	Public Key Infrastructure (PKI) governs the issuance of digital certificates to protect sensitive data, provide unique digital identities for users.
EPP - Endpoint Protection Platform	A comprehensive endpoint security solution specifically designed to protect individual devices.
XDR - Extended detection and response	A unified security solution that automatically collects, aggregates, and analyses data from multiple point products–email, endpoints, servers, cloud workloads, and networks
MDR - Managed Detection and Response	A security service that combines technology and human expertise to identify, investigate, and respond to threats on behalf of organisations.
NGIPS - Next-Generation Intrusion Prevention System	It is a security technology designed to monitor network traffic for malicious activity or security threats.
DNSSEC - Domain Name System Security Extensions	A suite of protocols that add cryptographic signatures to DNS responses, enabling resolvers to verify data integrity and authenticity.
NITDA-CERRT	A government cert, coordinating and facilitating information sharing, providing mitigation strategies and recommendations for incident response and recovery in Nigeria
HVAC - Heating, Ventilation, and Air Conditioning	A system designed to control the temperature, humidity, and air quality within residential and commercial buildings.

REFERENCES

Resource	Reference URL
Central Bank of Nigeria (CBN)	Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers: https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20exposure%20draft%20june.pdf
Securities and Exchange Board of India (SEBI)	Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (Circular No. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113; issued 20 August 2024): https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html SEBI
Center for Internet Security (CIS)	CIS Critical Security Controls v8.1: https://www.cisecurity.org/controls/v8 CIS Controls Resources: https://www.cisecurity.org/controls/resources
Government of Malaysia	Malaysia Cyber Security Strategy 2020–2024: https://www.nacsa.gov.my/
National Institute of Standards and Technology (NIST)	Cybersecurity Framework (CSF) 2.0: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf Cybersecurity Framework Resources: https://www.nist.gov/cyberframework

International Organization for Standardization (ISO)	ISO Standards Catalogue: https://www.iso.org/standards.html

ANNEXURE I

CYBERSECURITY INCIDENT/BREACH NOTIFICATION TEMPLATE

(To be submitted to NCC and the Cybercrime Advisory Council)

1. Reporting Organization Information

Organization Name	
Sector/Tier	
Physical Address	
Contact Person	
Designation	
Phone Number/Email	

2. Incident Details

Incident Title	
Date & Time Detected	
Date & Time Occurred (if known)	
Detection Method (e.g., SIEM, User Report)	
Type of Incident (e.g., DDoS, Ransomware)	
Systems Affected	
Severity Level (☐ Critical ☐ High ☐ Medium ☐ Low)	
Estimated Data/Asset Impacted	

3. Description of Incident

Provide a brief narrative of what happened, how it was discovered, systems affected, and potential implications.

4. Initial Response and Containment Measures

Detail the immediate steps taken to contain and mitigate the breach.

5. Investigation and Root Cause Analysis (if available)

Summarize findings from preliminary investigations (if concluded).

6. Recovery Measures and Current Status

Describe recovery actions taken, systems restored, and whether normal operations have resumed.

7. Notifications Made

Entity	Date Notified	Method of Notification	Reference No.
NCC			
ngCERT			
Other Agencies (if applicable)			

8. Additional Comments or Requests

E.g., assistance needed, collaboration request, technical support.

9. Declaration

I hereby certify that the above information is accurate to the best of my knowledge, and this notification is submitted in compliance with the Nigerian Cyber Risk Framework for the Communications Sector.

Name	Designation	Signature	Date

ANNEXURE II

SERVICE PROVIDER TIERS

#	CATEGORY
TIER 1 - *Service Providers who own, lease, and/or operate core networks, have leased spectrum resources, and all entities providing any form of communication service in Nigeria*	
1	UASL - Universal Access Service License
2	International Cable Infrastructure & Landing Station license
3	Data Centre owners & Operators
4	Clearing House
5	IGW – International Gateway
6	IDA – International Data Access
7	IXP – Internet Exchange Point
8	MFCN - Metropolitan Fibre Cable Network
9	Global Mobile Personal Communications by Satellite (GMPCS)
10	Full Gateway Services (FGS)
TIER 2 - *Service Providers with national coverage, aggregate service, provide shared infrastructure, and other emerging technology service providers*	
1	ISPs – Internet Service Providers
2	IOT Device Solutions (AVTSS, etc.)
3	PNL – Private Network License
4	VAS Aggregators
5	Metro Fibre Cable
6	National Long-Distance Operator
7	A2P – Application to Phone
8	VAS contents
9	Paging
10	Commercial Basic Radio Communications Network Services
11	Trunk Radio Networks
12	Collocation/Infrastructure Sharing Services
13	National Long-Distance Operator (NLDO)
14	Mobile Number Portability
TIER 3 - *All other Service providers who provide support services to other communication service providers*	
1	Sales & Installation of Terminal Equipment
2	Open Access Fibre Infrastructure

3	Automated Vehicle Tracking Services (AVTS)
4	Cabling
5	Cyber Café
6	Tele-Centre
7	Public Payphone
8	Non-Commercial/Closed User Radio Networks for Non-Telecoms Companies

ANNEXURE III

SCOPE DEFINITION FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

This annexure provides a standardized template for defining the scope of Vulnerability Assessment and Penetration Testing (VAPT) for the service providers. It ensures uniformity in planning, implementation, and reporting of security testing activities.

1. Objectives of the VAPT Exercise

i. Identify vulnerabilities in IT infrastructure, applications, and systems.
ii. Simulate real-world cyber-attacks to assess the resilience of critical assets.
iii. Test the effectiveness of security controls and incident detection capabilities.
iv. Recommend corrective actions to strengthen cyber defenses.

2. In-Scope Components

Component	Description
Network Infrastructure	Switches, routers, firewalls, load balancers, VPN gateways.
Public-Facing Applications	Websites, APIs, portals, and mobile applications.
Internal Business Applications	CRM, ERP, HRM, and other enterprise systems.
Cloud Infrastructure	IaaS, PaaS, SaaS platforms used for operations.
Endpoints and Access Devices	Laptops, desktops, mobile phones, remote terminals.
Databases and Repositories	SQL/NoSQL databases, data lakes, file systems.
Identity and Access Management	Active Directory, SSO, MFA, access control systems.
Monitoring and Logging Tools	SIEM, IDS/IPS, log servers, antivirus/EDR solutions.

3. Out-of-Scope Components

The following components are excluded from the VAPT exercise unless otherwise approved in writing:

- Legacy platforms that may be disrupted by testing.
- Production SCADA/ICS systems unless in test-safe environments.
- Third-party systems without formal authorization.
- Any systems not owned, controlled, or managed by the entity.

4. Testing Methodology and Approach

- Conduct automated and manual vulnerability scanning.
- Perform controlled penetration testing against in-scope components.
- Categorize and prioritize risks using CVSS and business impact analysis.
- Coordinate testing to avoid disruption and ensure safe execution.

5. Reporting Requirements

The VAPT final report must include:

- Executive summary with findings and recommendations.
- Technical report detailing vulnerabilities, risk levels, and evidence.
- Risk matrix and impact likelihood summary.
- Compliance mapping against applicable standards and policies.
- Signed attestation of test scope, method, and tester credentials.

ANNEXURE IV

STANDARD OPERATING PROCEDURE (SOP) FOR INCIDENT REPORTING TO NCC-CSIRT

1. Purpose

This SOP provides clear guidance for licensed operators, service providers, and related stakeholders in reporting cybersecurity incidents to the Nigerian Communications Commission – Computer Security Incident Response Team (NCC-CSIRT). It ensures timely, consistent, and accurate communication and enables a coordinated response to cybersecurity threats within the communications industry.

2. Scope

This procedure applies to all Tier 1, Tier 2, and Tier 3 operators under NCC jurisdiction, including Mobile Network Operators (MNOs), ISPs, MVNOs, Infrastructure Providers, and Data Centres operating within Nigeria.

3. Incident Classification

Incidents must be categorized according to the following severity levels:

- **Critical:** National impact, data breach involving sensitive personal information, system-wide outage.
- **High**: Service disruption to multiple users, attempted large-scale attack.
- **Medium**: Targeted attacks, malware infections, and misconfigurations with risk exposure.
- **Low**: Isolated or non-impacting security observations.

4. Reporting Timelines

The framework will adopt a two-step reporting approach as follows:

- Reporting timeline for detection - 4 Hours
- The confirmation reporting timeline - 24 hours, with periodic 4-hour updates after the first detection.

5. Reporting Channels

Incidents must be reported via one or more of the following channels:

- Email: incident@csirt.ncc.gov.ng
- Web Portal: *https://csirt.ncc.gov.ng*

- Phone Number: +234-2094617422
- Physical Submission (where necessary) to the NCC-CSIRT Office.

6. Incident Report Content

The submitted incident report should include:

- Name and contact of reporting entity.
- Incident type, classification, and detection method.
- Date/time of occurrence and discovery.
- Systems and services affected.
- Preliminary assessment of impact.
- Response measures already taken.
- Any suspected attribution or root cause (if known).
- Any other relevant information

7. Escalation Protocols

If an incident escalates beyond initial severity classification or poses broader systemic risks, NCC-CSIRT should be updated immediately using the fastest available communication channel. Further coordination with sectoral CSIRTs, ngCERT, and law enforcement may be initiated.

8. Follow-Up and Closure

Within 7 days of initial notification, the reporting entity must submit a follow-up report containing:

- Post-incident analysis and lessons learned.
- Mitigation steps and updates on corrective actions.
- Final assessment of impact and restoration status.
- Updated contact information (if applicable).

9. Compliance Note

Failure to report incidents within the specified timeframes may result in sanctions or penalties in accordance with applicable NCC regulations and the CRF-NCS.

ANNEXURE V

SECURITY CONTROLS FOR CUSTOMER-FACING APPLICATIONS

1. Objectives of the Exercise

This annexure outlines the mandatory and recommended security controls for customer-facing applications within the Nigerian Communications Industry. These controls are aimed at safeguarding user data, ensuring system availability, and maintaining the confidentiality, integrity, and trust of digital services offered to consumers.

2. Scope

This annexure applies to all internet-facing applications, including:

- Websites and portals
- Online billing and self-service platforms
- Mobile applications (Android/iOS)
- Customer account management systems
- APIs and other interfaces exposed to end users

3. Security Control Domains

Control Area	Control Description	Applicability
Authentication & Access	Enforce Multi-Factor Authentication (MFA) for both users and administrators.	All tiers
Input Validation	Use strict server-side validation to protect against XSS, SQLi, and command injections.	All tiers
Session Management	Implement secure cookies (Http Only, Secure), session timeouts, and token expiration.	All tiers
Data Encryption	Enforce HTTPS (TLS 1.2 or higher); encrypt	All tiers

	sensitive data at rest with AES-256.	
Secure Coding	Adopt OWASP Top 10 secure coding practices across all development teams.	All tiers
API Security	Protect APIs with OAuth 2.0, rate limiting, and strong input validation.	Tier 1 & 2
Logging & Monitoring	Enable centralized logging, anomaly detection, and integrate logs with SIEM tools.	All tiers
Access Control	Role-based access control (RBAC) should be implemented for both users and systems.	All tiers
Patch Management	Apply regular updates to server software, libraries, and CMS platforms.	All tiers
Security Testing	Conduct regular vulnerability scanning, penetration testing, and code audits.	All tiers
Privacy by Design	Integrate user data privacy mechanisms (e.g., consent prompts, masking).	All tiers
Incident Integration	Ensure logs and alerts feed into incident response platforms (e.g., SIEM, CSIRT).	Tier 1 & 2
Change Management	Deploy secure DevOps practices; document and review all changes before release.	All tiers

4. Minimum Compliance Requirements

- Must meet the applicable NCC cybersecurity baseline controls.
- Align with industry frameworks such as OWASP ASVS, ISO/IEC 27034, and NIST SP 800-53.
- Tier 1 service providers must submit an annual security attestation report for customer-facing platforms.

5. Review Frequency

Security controls must be reviewed:

- At least Biannually
- As required
- After any significant incident
- Following major application or infrastructure changes

ANNEXURE VI

ENCRYPTION GUIDELINES FOR DATA AT REST

1. Objectives of the Exercise

This annexure establishes minimum requirements and best practices for the encryption of data at rest across the Nigerian Communications Industry. It aims to ensure that sensitive and critical information stored on physical or virtual media is protected from unauthorized access, tampering, or theft in accordance with the Cyber Risk Framework and applicable data protection laws.

2. Scope

This guideline applies to:

- All regulated entities (Tier 1–3).
- Data stored on databases, servers, hard drives, storage area networks (SAN), cloud platforms, portable media, and backup devices.
- Sensitive, confidential, or regulated data including Personally Identifiable Information (PII), customer data, credentials, logs, financial data, and critical system configurations.

3. Encryption Requirements

Control Area	Guideline	Applicability
Encryption Algorithm	Use AES-256 or equivalent NIST-approved algorithms for all sensitive data at rest.	All tiers
Key Management	Implement centralized key management systems (KMS); separate encryption keys from data.	Tier 1 & 2
Access Control to Keys	Restrict key access to authorized personnel using RBAC and	All tiers

	enforce MFA on key stores.	
Tokenization/Masking	Apply tokenization for regulated data such as PAN, BVN, and National ID where applicable.	Tier 1 & 2
Database Encryption	Encrypt structured data (e.g., MySQL, PostgreSQL) using native or transparent encryption.	All tiers
Cloud Storage Encryption	Ensure cloud-stored data is encrypted using CSP-native or BYOK encryption models.	All tiers
Portable Media Encryption	Mandate full-disk encryption for USB drives, external HDDs, and laptops.	All tiers
Backup Encryption	All backups must be encrypted at rest with access and audit controls in place.	All tiers
Logs and Audit Trails	Encrypt log files that contain sensitive metadata or operational details.	Tier 1 & 2
Integrity Protection	Use hash verification (e.g., SHA-2) to ensure encrypted data has not been tampered with.	All tiers

4. Key Management Guidelines

- Use Hardware Security Modules (HSMs) for high-assurance environments (Tier 1 service providers).
- Keys must be rotated at least every 12 months or upon suspected compromise.
- Encryption keys should never be hardcoded into applications or stored with encrypted data.

- Maintain audit logs of key creation, rotation, and access.

5. Compliance and Exceptions

- Service providers must demonstrate compliance during NCC audits or on request.
- Any exception to these guidelines must be formally documented, justified, and approved by NCC prior to implementation.

6. Review and Updates

These encryption guidelines shall be reviewed at least Biannually or following any major regulatory, technological, or threat landscape changes.

ANNEXURE VII

SECURITY MEASURES FOR DATA TRANSMISSION OVER THE INTERNET

1. Purpose

This annexure outlines the minimum required security measures to protect data transmitted over the internet by licensed service providers in Nigeria's communications industry. These measures are designed to ensure data confidentiality, integrity, and authenticity during transmission, and to reduce the risk of interception, tampering, or man-in-the-middle (MitM) attacks.

2. Scope

These guidelines apply to all:

- Data flows between internal systems and external endpoints over public networks.
- APIs, customer portals, mobile/web applications, email, and remote administration interfaces.
- Communications involving Personally Identifiable Information (PII), authentication credentials, sensitive transactions, or regulated datasets.

3. Mandatory Controls

Control Area	Security Measure	Applicability
Transport Encryption	Use TLS 1.2 or higher (preferably TLS 1.3) for all HTTPS connections and encrypted email protocols.	All tiers
Certificate Management	Use valid, non-expired SSL/TLS certificates from a trusted CA; implement manual monitoring,	All tiers

	centralised inventory, automated alerts and quarterly reviews.	
API Security	Use secure authentication mechanisms (OAuth 2.0, JWT, API keys with expiry); apply rate limiting.	Tier 1 & 2
DNS Security	Implement DNSSEC and secure DNS resolvers to mitigate DNS spoofing risks.	Tier 1 & 2
Email Security	Enable STARTTLS, DKIM, SPF, and DMARC to secure outbound and inbound emails.	All tiers
Remote Access	Enforce VPN or Zero Trust Network Access (ZTNA) for administrative access over the internet.	All tiers
File Transfer Security	Use SFTP or HTTPS for secure file exchanges; prohibit use of unsecured FTP/HTTP.	All tiers
End-to-End Encryption (E2EE)	Where feasible, adopt E2EE for sensitive customer messaging platforms or service portals.	Tier 1
Session Security	Use strong session identifiers, encryption of tokens, and session timeouts.	All tiers

Monitoring and Logging	Monitor encrypted connections for anomalies; log failed TLS handshakes and expired certs.	Tier 1 & 2

4. Key Best Practices

- Avoid deprecated protocols such as SSLv3, TLS 1.0, or RC4 cipher suites.
- Disable insecure ports/services unless absolutely required (e.g., Telnet, FTP).
- Regularly test and validate secure transmission using penetration testing tools or SSL scanners.
- Educate developers and infrastructure teams on secure transport configurations and updates.

5. Compliance Monitoring

Service providers must demonstrate compliance with these measures during NCC audits or reviews. Exceptions must be documented, risk-assessed, and approved in writing by the appropriate authority.

6. Review and Updates

This annexure should be reviewed and updated at least biannually or following the release of new transmission security standards or industry guidance.

ANNEXURE VIII

ENCRYPTION STANDARDS FOR DATA IN CLOUD ENVIRONMENTS

1. Purpose

This annexure outlines mandatory encryption standards for safeguarding sensitive and regulated data stored, processed, or transmitted within cloud environments. It ensures data confidentiality, integrity, and availability in line with Nigeria's cybersecurity framework for the communications sector.

2. Scope

These standards apply to:

- All Tier 1–3 service providers using public, private, hybrid, or multi-cloud services.
- Data at rest, in transit, and during processing in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) models.
- Sensitive data including Personally Identifiable Information (PII), service configurations, logs, customer records, and authentication credentials.

3. Encryption Requirements

Control Area	Requirement	Applicability
Encryption Algorithm	Use AES-256 or equivalent NIST-approved algorithms for data at rest.	All tiers
Data in Transit	Use TLS 1.2+ or equivalent for all communications between systems, APIs, and cloud services.	All tiers
Key Management	Implement centralized Key Management Systems (KMS); support BYOK (Bring	Tier 1 & 2

	Your Own Key) or HYOK.	
Customer Data Isolation	Ensure logical separation of customer data using encryption and access policies in shared environments.	All tiers
Storage Encryption	Enable encryption on all cloud storage (e.g., S3 buckets, disks, blobs, snapshots).	All tiers
Database Encryption	Use Transparent Data Encryption (TDE) for cloud-managed databases.	All tiers
API Protection	Sign/encrypt API calls using secure tokens or digital signatures.	Tier 1 & 2
Access to Keys	Restrict access to encryption keys using RBAC and enable auditing.	All tiers
Backup Encryption	Enforce encryption of all cloud-stored backups and snapshots.	All tiers
Tokenization/Masking	Use tokenization or masking for sensitive data where full encryption is not required.	Tier 1 & 2

4. Cloud Provider Requirements

- These standards apply to:
- All Tier 1–3 service providers using public, private, hybrid, or multi-cloud services.
- Data at rest, in transit, and during processing in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) models.
- Sensitive data including Personally Identifiable Information (PII), service configurations, logs, customer records, and authentication credentials.

5. Audit and Compliance

Service providers must:

- Document their encryption implementation strategy.
- Provide evidence of encryption during security assessments or audits.
- Review and rotate encryption keys at least annually or as per policy.
- Continuously review encryption performance against Quantum Secure Cryptography

6. Review and Update

This annexure shall be reviewed biannually, or upon major technological or policy changes affecting cloud encryption practices.

ANNEXURE IX

LIST OF LICENSE CATEGORIES

#	CATEGORY
	CLASS LICENSE
1	Sales & Installation of Terminal Equipment
2	Repairs & Maintenance of Telecom Facilities
3	Cabling
4	Cyber Café
5	Tele-Centre
6	Public Payphone
	INDIVIDUAL LICENSE
1	Sales & Installation of Terminal Equipment (S & I)
2	Value Added Services
3	Automated Vehicle Tracking Services (AVTS)
4	Internet Services (ISP)
5	Paging
6	Commercial Basic Radio Communications Network Services
7	Trunk Radio Networks
8	Collocation/Infrastructure Sharing Services
9	Internet Exchange Services
10	Private Network Links (PNL) Local Exchange Operator (Cable Only)
11	PNL Regional
12	Global Mobile Personal Communications by Satellite (GMPCS)
13	Metropolitan Fibre Cable Network (MFCN)
14	Full Gateway Services (FGS)
15	National Long Distance Operator (NLDO)
16	Open Access Fibre Infrastructure
17	Unified Access Service (UASL: Fixed Telephony National/Regional, DML, RLDO, NLDO, IDA, FGS)
18	Non-Commercial/Closed User Radio Networks for Non-Telecoms Companies
19	International Cable Infrastructure & Landing Station Licence
20	Mobile Number Portability

ANNEXURE X

KEY PERFORMANCE INDICATORS, MEASUREMENTS, AND TARGETS FOR CYBER RESILIENCE FRAMEWORK FOR COMMUNICATION SECTOR (CRF-NCS)

CATEGORY	KPIs	MEASURE	MEASUREMENT	TARGET	MEASUREMENT TIMELINE
CATEGORY 1: REGULATORY MATURITY	Impact on Global Cybersecurity Index	Progress on Global Cybersecurity Rating (GCI)	Global index assessing country preparedness to prevent cyber threats and manage incidents	50% Progress	Bi-annual
	Framework Enforcement Rate	Regulatory follow-through	Percentage of reported non-compliant cases actioned	100%	Quarterly
	Framework Satisfaction Score	Feedback on usability and support for framework	Survey results from service providers	≥ 80% positive feedback	Annual
	Industry Cybersecurity Awareness Rate	Sectoral Cybersecurity Awareness	Survey results from service providers	≥ 50% of service provider staff trained on cybersecurity	Annual

CATEGORY 2: INCIDENT DETECTION, RESPONSE, AND BUSINESS CONTINUITY	BCP/DRP Testing Frequency	Regular testing of recovery plans	Percentage of service providers conducting tests	100% (Tier 1), ≥ 80% (Tier 2)	Annual
	Time to Recovery (TTR)	Recovery efficiency after disruptions	Average time to restore operations	≤ 24 hours for critical services	Ongoing measurement Weekly reporting
	Incident Escalation Compliance Rate	Timely reporting to relevant authorities	Time to report incidents to NCC-CSIRT	≥ 95% compliance	Ongoing measurement Weekly reporting
	Infrastructure End of Life (EoL)	Legacy infrastructure management	Rate of decommissioning outdated systems	≤ 20% of infrastructure with EoL	Decommissioning phased over 12-36 months
	Service Availability for CII	Critical service uptime	Percentage of time critical telecom services are available	≥ 95% availability	Ongoing measurement Weekly reporting
CATEGORY 3: RISK IDENTIFICATION,	Risk Register Maturity Score	Maintenance of risk registers	Percentage of service providers with updated risk registers	≥ 90% of Tiers 1 & 2 service providers	Quarterly

ASSESSMENT, & MONITORING	Annual Risk Assessment Completion Rate	Comprehensive risk evaluation	Percentage of completed annual assessments	100% (Tier 1), ≥80% (others)	Annual
CATEGORY 4: SECTOR-WIDE THREAT INTELLIGENCE AND COLLABORATION	Threat Bulletin Impact Rate	Impact of threat bulletin on service availability	Survey results from service providers	≥ 80% Positive Impact	Annual
	Threat Intelligence Contribution Index	Collaborative defense posture	Percentage of licensees contributing threat data	≥ 70% By Year 2	Annual
	Regulatory Escalation Response Time	Responsiveness to reported cyber security issues	Average time for NCC to respond	≤ 48 hours	Immediate/real-time
CATEGORY 5: IMPLEMENTATION OF CONTROLS	Security Control Implementation Index	Implementation of recommended controls	Percentage of controls implemented	≥ 85% (Tier 1), 70% (Tier 2)	Ongoing measurement Monthly reporting
	Patch and Vulnerability Closure Rate	Vulnerability management	Average time to close critical vulnerabilities	Between 5 - 15 days (Depends on severity)	Ongoing measurement Monthly reporting

CATEGORY 6: CROSS SECTOR COLLABORATION, SECTORAL AUDIT & COMPLIANCE	Ecosystem and Cross Sector Collaboration Rate	Collaboration with related entities	Signed collaboration agreements	At least one agreement with Cross sector, national, regional and international organisation	Bi-annual

ANNEXURE XI

CYBER RESILIENCE FRAMEWORK FOR NIGERIA COMMUNICATION SECTOR (CRF-NCS) OBJECTIVES AND STANDARDS

PILLAR	PILLAR ELEMENTS	OBJECTIVES	STANDARDS
PILLAR 1: GOVERNANCE AND COMPLIANCE (GC)	**GC-LR: Laws and Regulations**	This control objective specifies the requirements for compliance with all relevant legal and regulatory frameworks as applicable in Nigeria.	1. **(GC-LR.S1)** Legal and regulatory requirements of the Nigeria Cybercrime (Prevention, Prohibition, etc) (Amendment) Act 2024 regarding the designation and protection of Critical National Information Infrastructure (CNII), cybersecurity, including data protection and data privacy, shall be understood, managed, and complied with. 2. **(GC-LR.S2)** Provisions of the National Cybersecurity Policy and Strategy 2021 regarding cybersecurity and the designation and protection of Critical National Information Infrastructure (CNII) shall be understood, managed, and complied with.

			3. **(GC-LR.S3)** Legal and regulatory requirements of the Nigeria Data Protection Act 2023 regarding data protection and data privacy shall be understood, managed, and complied with. 4. **(GC-LR.S4)** Provisions of the Nigerian Communications Act of 2003 and its subsidiary legislations shall be understood, managed, and complied with. 5. **(GC-LR.S5)** The regulator and service providers shall comply with the provisions of the official gazette on the designation and protection of CNII order, 2024, and shall be understood, managed, and complied with.
	GC-SE: Sector Environment	This control objective evaluates whether service providers have a comprehensive	1. **(GC-SE.S1)** Key sector service providers understand the most urgent cybersecurity risks to their organisations, systems, and critical assets—risks that also threaten the sector's overall functioning. This includes

		understanding of the sector's cybersecurity challenges, objectives, and priorities. It includes their awareness of key stakeholders, as well as their roles, responsibilities, and activities. Additionally, it assesses whether this awareness influences their actions and decision-making, thereby impacting	awareness of emerging threats and vulnerabilities stemming from digitalization and the integration of digital technologies into networked infrastructure. 2. **(GC-SE.S2)** The roles of service providers in operating and maintaining critical systems and infrastructure within their industry sector are clearly identified and conveyed. 3. **(GC-SE.S3)** Dependencies and critical functions essential for delivering critical services are identified and effectively managed. 4. **(GC-SE.S4)** Service providers understand the resilience requirements necessary to maintain the delivery of critical services across all operating conditions, including under duress or attack, during recovery, and during normal operations.

		the cybersecurity posture of their organisations and, consequently, the entire sector.	5. **(GC-SE.S5)** Service providers understand the Cyber risk of having refurbished, end-of-life, end-of-sales, non-type-approved equipment in their networks. 6. **(GC-SE.S6)** Service providers mitigate cybersecurity risks by communicating and collaborating with peers, vendors, service providers, NCC, and National Authorities like the Office of the National Security Adviser (ONSA), National Cyber Security Coordination Centre (NCCC), Nigeria Police Force (NPF-CCC), Department of State Services (DSS), etc.
	GC-RRA: Roles, Responsibilities and Authorities	This control objective emphasizes the importance of defining and communicating	1. **(GC-RRA.S1)** The leadership of the service provider (Board or executive management) bears the responsibility and accountability for cybersecurity risk. They are tasked with fostering a culture that is risk-aware,

		cybersecurity roles, responsibilities, and authorities to promote accountability, facilitate performance evaluation, and support ongoing improvement.	cybersecurity-conscious, and dedicated to continuous improvement. 2. **(GC-RRA.S2)** Cybersecurity risk management roles, responsibilities, and authorities shall be developed, communicated, understood, and enforced. 3. **(GC-RRA.S3)** A CISO or designated officer shall be appointed and shall report to leadership. They are responsible for coordinating, developing, implementing, and maintaining the organisation's overall cybersecurity strategy, plan, program, and activities. 4. **(GC-RRA.S4)** The CISO or headship of the information security function must have requisite qualifications, skills and experience. Service Providers must notify the Nigerian Communications Commission of the appointment of a CISO.

			5. **(GC-RRA.S5)** Noting the dynamics within the sector, where possible, there should be alternate CISOs to ensure leadership continuity (in the event of the primary CISO not being available), for organisations with multiple sites/locations, for succession planning, and work distribution. 6. **(GC-RRA.S7)** Cybersecurity shall be included in human resources training programs during staff on-boarding and on an on-going basis. 7. **(GC-RRA.S8)** The service provider relies on a dedicated sectoral NCC-CSIRT which functions as the single point of contact for the sector. This team is responsible for overseeing sector-specific IT security, monitoring and analyzing cyber threats, and issuing warnings and alerts regarding potential or ongoing attacks. Additionally, it

			coordinates incident response and investigations, conducts cybersecurity awareness and educational programs for sector stakeholders, and integrates its capabilities into the larger national cybersecurity ecosystem as appropriate.
	GC-PP: Policies and Procedures	This control objective evaluates whether service providers have developed specific policies and procedures to formalize their cybersecurity governance. It particularly focuses on whether these policies and	1. **(GC-PP.S1)** A comprehensive cybersecurity and cyber resilience policy shall be documented and implemented following approval from the leadership of the service provider. 2. **(GC-PP.S2)** The cybersecurity and cyber resilience policy shall incorporate industry best practices and include the standards and guidelines outlined in this framework. 3. **(GC-PP.S3)** The cybersecurity and cyber resilience policy shall be reviewed periodically by the service providers.

		procedures align with cybersecurity requirements set by the sectoral regulator and if their implementation and effectiveness are regularly monitored.	4. **(GC-PP.S4)** A policy for managing cybersecurity risks shall be established, tailored to the organisational context, cybersecurity strategy, and priorities. This policy shall be communicated and enforced within the service provider organisation. 5. **(GC-PP.S5)** The cybersecurity risk policy shall be reviewed regularly, updated as needed, communicated to relevant stakeholders, and enforced to ensure continuous improvement and adaptation to evolving requirements, threats, and technologies. 6. **(GC-PP.S6)** A clear definition of ownership and custodianship for each asset, along with a structured chain of command for obtaining approvals, shall be established and strictly followed.

			7. **(GC-PP.S7)** The service provider must comply with the sector's cybersecurity regulations, requirements, directives, and guidelines (e.g., Executive Order on CNII protection; requirements on incident reporting for CNIIs; cybersecurity responsibilities for essential services; voluntary or mandatory baseline cybersecurity performance goals). 8. **(GC-PP.S8)** Service providers should implement cybersecurity good practices even when not required.
	GC-O: Oversight	This control objective highlights the importance of using the results of organisation-wide cybersecurity risk management	1. **(GC-O.S1)** The outcomes of the cybersecurity risk management strategy are regularly evaluated to improve and refine strategic decisions and guide future directions. 2. **(GC-O.S2)** The cybersecurity risk management strategy undergoes periodic

		activities, performance, and outcomes to inform, improve, and refine the risk management strategy.	review and refinement to maintain comprehensive coverage of organisational requirements and emerging risks. 3. **(GC-O.S3)** Organisational cybersecurity risk management performance is assessed and refined as needed to ensure effectiveness and alignment with evolving risks. 4. **(GC-O.S4)** Organisations should periodically evaluate their cyber resilience posture through the Cybersecurity Capability Index (CCI).
	GC-SCRM: Supply Chain Risk Management	The control objective outlines the priorities, constraints, risk tolerance, and assumptions to inform decision-making in managing	1. **(GC-SCRM.S1)** Service providers shall define and communicate their roles in managing ICT supply chain risks both internally and externally to NCC and relevant stakeholders (where necessary). 2. **(GC-SCRM.S2)** The cybersecurity supply chain risk management strategy and processes shall be clearly defined,

		supply chain risks. The service provider has implemented processes to effectively identify, assess, and mitigate these risks.	implemented, regularly evaluated, and effectively managed with the consensus of organisational stakeholders. 3. **(GC-SCRM.S3)** Employees and third-party service providers shall be granted access to the service provider's information systems only after they have signed confidentiality and product/service integrity agreements. 4. **(GC-SCRM.S4)** Suppliers and third-party service providers of information systems, hardware, network components, and services must be identified, prioritized, and assessed through a thorough cybersecurity supply chain risk assessment process. 5. **(GC-SCRM.S5)** Contracts with suppliers and third-party service providers must include essential measures to align with the service provider's cybersecurity objectives and supply chain risk management plan.

			6. **(GC-SCRM.S6)** Service providers must continuously monitor, review, and verify adherence of suppliers and third-party service providers to the NCC Cybersecurity framework to ensure ongoing security and operational integrity of services provided. 7. **(GC-SCRM.S7)** For all new software acquisitions related to core and critical service provider activities, a Software Bill of Materials (SBOM) must be obtained and maintained with each upgrade or modification. If obtaining an SBOM is not feasible for legacy or proprietary systems, approval must be obtained from the leadership of the service provider, accompanied by documented limitations, the rationale for non-obtaining, and a comprehensive risk management plan for these systems.

			8. **(GC-SCRM.S8)** Response and recovery plans, along with testing, must be conducted in collaboration with third-party service providers to ensure coordinated incident management and resilience of the product or service provided by the third party. 9. **(GC-SCRM.S9)** The concentration risk associated with outsourced organisations must be evaluated and periodically reviewed to enhance operational resilience. 10. **(GC-SCRM.S10)** Third-party service providers must comply with the same information security standards as the service providers to ensure consistency and uniformity across all operations. 11. **(GC-SCRM.S11)** Service providers must establish strong supply chain and procurement controls to ensure that their

			services comply with legal requirements and regulatory standards. 12. **(GC-SCRM.S12)** Service providers must implement strong controls for third-party access and outsourcing to effectively manage the risks involved in sharing information and working with external partners. 13. **(GC-SCRM.S13)** Service providers shall be required to comply with internationally recognised standards and frameworks on supply chain risk management.
	GC-BS: Budget and Spending	This control objective assesses whether service providers have access to dedicated financial resources and whether those	1. **(GC-BS.S1)** Budgetary planning process shall be aligned with information security and privacy management objectives and processes. Adequate resources shall be allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies.

		resources are allocated to support cybersecurity efforts in their organisation.	2. **(GC-BS.S2)** Service providers have access to dedicated financial resources, which shall be formally allocated to strengthen cybersecurity measures and initiatives. 3. **(GC-BS.S3)** The service provider's cybersecurity budget is strategically allocated to align with specific cybersecurity objectives and their associated implementation activities. 4. **(GC-BS.S4)** The service provider tracks cybersecurity budget expenditures and adjusts future budgets as needed to ensure optimal resource allocation and enhance security effectiveness.
	GC-RM: Risk Management Strategy	This control objective assesses whether service providers have a	1. **(GC-RM.S1)** The service provider's priorities, constraints, risk tolerance, risk appetite statements, assumptions, and limitations are clearly defined, effectively

		clear understanding of their assets, especially the most critical ones, and their status. It also assesses the service provider's awareness of the potential impact of adverse events on these assets, as well as their understanding of the interrelationships between these assets. Additionally, it considers whether this knowledge is	communicated, and actively used to inform operational risk decision-making. 2. **(GC-RM.S2)** Service providers must establish a cyber risk management framework to identify, assess, mitigate, and monitor risks, supported by clearly defined security processes and procedures. Cyber risk management objectives should be clearly defined and agreed upon by all relevant stakeholders. 3. **(GC-RM.S3)** Different risk scenarios and their corresponding treatment must be documented and regularly tested to assess and improve the service provider's risk management plan. 4. **(GC-RM.S4)** Risk tolerance and risk appetite statements must be clearly defined, effectively communicated, and consistently maintained. Service providers should

		regularly reviewed and updated	establish and articulate their acceptable risk levels to support informed and consistent decision-making. 5. **(GC-RM.S5)** The service provider's risk tolerance should be established based on their role in critical infrastructure and sector-specific risk assessments. A risk register must be maintained and periodically reviewed and approved by management or the appropriate Board Committee.
	GC-C: Compliance	This control objective helps service providers stay up to date with evolving regulations and implement necessary measures to comply with	1. **(GC-C.S1)** Information Technology (IT) audit and security compliance reports must be submitted biannually to the leadership of the service provider to support informed decision-making. 2. **(GC-C.S2)** Service providers shall put in place appropriate systems and procedures to ensure compliance with the provisions

		them. By achieving and maintaining compliance, this control objective helps service providers avoid penalties, legal liabilities, and reputational damage.	(i.e., applicable standards and guidelines) of the CRF-NCS. 3. **(GC-C.S3)** Service providers shall conduct self cyber audit as per CRF-NCS at the stipulated timelines and cyber audit reports along with other required documents shall be submitted to NCC in accordance with the timelines provided in CRF-NCS. 4. **(GC-C.S4)** Service providers shall be required to comply with internationally recognised standards and cybersecurity frameworks as appropriate.
PILLR 2: CYBER RISK MANAGEMENT **CRM: Objectives:**	**CRM-AR: Asset and Risk Management**	The data, personnel, devices, systems, and facilities essential to the service provider's business operations	1. **(CRM-AR.S1)** Physical devices, digital assets (including URLs, domain names, IP addresses, applications, APIs, etc.), network resources and shared resources such as cloud assets, data, and other interfacing systems within the organisation are

1. The Cyber Risk Management (CRM) objective assesses service providers' awareness of their assets, especially the most critical ones, and their status. 2. It also evaluates their understanding of the potential impact of		are identified and managed consistently, based on their relative importance to organisational objectives and the service provider's overall risk strategy.	systematically inventoried within a defined timeframe. They are then classified based on their criticality and risk level. 2. **(CRM-AR.S2)** Organisational communication, data flows, and encryption methods shall be mapped and inventoried across all IT systems and network resources. 3. **(CRM-AR.S3)** Service providers shall ensure that no shadow IT/OT assets are present in the organisation. 4. **(CRM-AR.S4)** The leadership of the service provider shall approve the list of *critical systems* (hardware and software and network infrastructure) that are in use in the service provider environment. 5. **(CRM-AR.S5)** Inventories of data, and corresponding metadata for designated (critical) data types shall be maintained.

adverse events on these assets. 3. Additionally, it examines whether service providers have a comprehensive grasp of the relationships between their assets and ensures this knowledge is regularly updated.			6. **(CRM-AR.S6)** All inventoried IT/OT assets and data are managed throughout their lifecycles. 7. **(CRM-AR.S7)** The service provider shall develop or adopt a cyber risk management strategy/framework that includes regular assessments of the likelihood and impact of adverse events or attacks, along with defined measures to mitigate identified risks. 8. **(CRM-AR.S8)** The service provider shall ensure that its cyber risk management strategy is aligned with the common methodology defined at the sectoral and/or national level, enabling the seamless exchange of risk information through standardized taxonomies, normalization models, and related frameworks.

	CRM-SAIS: Situation Awareness and Information Sharing	This control objective evaluates whether key entities actively monitor relevant information to stay informed about the cybersecurity landscape, operational context, and vulnerabilities impacting their assets and systems. It also assesses the tools and methodologies used in these evaluations, as well as the effectiveness	1. **(CRM-SAIS.S1)** The service provider performs vulnerability assessments on its assets, especially when deploying new equipment, enabling ports, or adding new services. 2. **(CRM-SAIS.S2)** The service provider carries out penetration tests to identify and validate exploitable vulnerabilities, evaluate perimeter defenses, and verify the security of externally accessible applications. 3. **(CRM-SAIS.S3)** The service provider shall monitor vulnerabilities across IT and OT environments (when applicable). 4. **(CRM-SAIS.S4)** The service provider shall implement a structured patch and vulnerability management procedure to ensure timely identification and remediation of security risks especially after a production release.

		of communicating findings to appropriate stakeholders within the sector.	5. **(CRM-SAIS.S5)** The service provider shall implement and sustain mechanisms to receive intelligence on known threats, hardware and software vulnerabilities, intrusions, anomalies, and other relevant exploits, in order to ensure comprehensive risk assessment. 6. **(CRM-SAIS.S6)** The service provider has established a structured process for sharing information on identified threats, vulnerabilities, and exploitable assets—including data breaches—with relevant stakeholders, including executives, operations personnel, sectoral supervisory authorities, regulators, and the NCC-CSIRT. 7. **(CRM-SAIS.S7)** The Service Provider are encouraged to report cybersecurity incidents, even when such disclosures are not mandated by existing regulations, to

			enhance transparency and security awareness.
	CRM-RA: Risk Assessment	The service provider evaluates and comprehends cybersecurity risks affecting the organisation, its assets, and individuals, ensuring effective risk management and mitigation strategies.	1. **(CRM-RA.S1)** The service provider shall identify, validate, and document asset vulnerabilities while assessing and managing risk factors across all IT assets. 2. **(CRM-RA.S2)** The service provider shall conduct periodic risk assessments of its IT environment, including evaluations of Quantum cryptography and emerging cybersecurity risk (e.g., PQC - Post-Quantum Computing), to ensure proactive security management and mitigation strategies. 3. **(CRM-RA.S3)** Service providers are required to use PQC to develop, communicate, and enforce quantum-resistant cryptography. 4. **(CRM-RA.S4)** Service providers shall obtain Cyber Threat Intelligence (CTI) from credible

			and trusted information sources. Service providers shall continue to receive advisories from the NCC-CSIRT threat Intelligence platform. 5. **(CRM-RA.S5)** Threats, vulnerabilities, their likelihoods, and potential impacts shall be analysed to assess inherent risk and establish a prioritised approach to risk response. 6. **(CRM-RA.S6)** Vulnerabilities and cyber threats, particularly those concerning access and authentication, shall be identified, assessed for their likelihood, and documented along with their potential business impacts. 7. **(CRM-RA.S7)** Risk responses shall be selected, prioritised, planned, monitored, and effectively communicated to ensure comprehensive risk management.

			8. **(CRM-RA.S8)** Valid cybersecurity insurance shall be maintained for critical assets to ensure comprehensive risk mitigation and financial loss protection.
PILLAR 3: CYBERSECURITY MEASURES **CM: Objective** This control objective assesses the technical and organisational strategies that key entities have put in place to address cybersecurity risks. These cybersecurity	**CM-DP: Data Privacy**	This control objective should align with national policy, industry regulation, and relevant legislation(s). These will inform local data management principles.	1. **(CM-DP.S1)** access to physical and logical assets and associated facilities is limited to authorised users, processes and devices, and is managed in accordance with the assessed risk of unauthorised access. 2. **(CM-DP.S2)** The service provider implements technical and organisational measures to safeguard data within its systems, ensuring confidentiality, integrity, and availability. These measures may include encryption, data loss prevention, regular backups, and logical or physical separation from data sources.

measures encompass controls related to Data Protection, Identity and Access Management, Network Security, Personnel Security, Endpoint Security, and cyber-hygiene practices.			3. **(CM-DP.S3)** The service provider shall meet all relevant provisions of the Nigeria Data Protection Act (NDPA) 2023 regarding Personally Identifiable Information (PII). 4. **(CM-DP.S4)** The service provider shall meet all requirements as contained in the Freedom of Information (FOI) Act (2011). 5. **(CM-DP.S5)** The service provider shall comply with Privacy by Design (PbD) industry best practice principles.
	CM-DS: Data Security	This control objective defines measures for managing information and records (data) consistent with the organisation's risk	1. **(CM-DS.S1)** Data-at-rest, Data-in-transit and Data-in-use shall be protected. Strong data protection measures (for at-rest, in-transit data and in-use data), with industry standard encryption algorithms, shall be put in place by all service providers. 2. **(CM-DS.S2)** Service providers must ensure that data related to reporting compliance

		strategy to protect the *Confidentiality, Integrity, and Availability* of information.	with this framework must be kept readily available, easily accessible, and in a readable and usable format within the legal jurisdiction of Nigeria. 3. **(CM-DS.S3)** Service providers shall maintain adequate capacity to ensure the availability of data. 4. **(CM-DS.S4)** Service providers shall implement measures to prevent data leaks/exfiltration. Appropriate tools shall be put in place to prevent and safeguard against any data leakage/exfiltration. 5. **(CM-DS.S5)** Development and testing environments must be separated from the production environment. For critical software or application development, at least one non-production environment must be used to conduct thorough testing before deployment to the production environment.

			6. **(CM-DS.S6)** Service providers shall be required to establish mechanisms to verify the integrity of hardware, software, firmware, and other systems connected to or reliant on their critical systems.
	CM-IDAM: Identity & Access Management	This control objective outlines measures for managing the digital identities, accounts, credentials, and authentication mechanisms of personnel. It includes practices such as assigning unique accounts, enforcing need-to-	1. **(CM-IDAM.S1)** Service providers shall **implement measures** to ensure the entire lifecycle of **identities and credentials** from **issuance and management to verification, revocation, and auditing** is securely handled for all **authorised devices, users, and processes**. 2. **(CM-IDAM.S2)** The service provider shall implement measures to **protect network integrity,** employing strategies like **network segregation** and **network segmentation** etc.).

		know, least privilege, and separation of duties principles, as well as implementing secure provisioning and deprovisioning processes, strong credentials, and multifactor authentication.	3. **(CM-IDAM.S3)** The service provider shall implement measures to ensure **access permissions and authorizations** to both **on-premises and cloud resources** are granted based on the **Principle of Least Privilege** and **segregation of duties.** 4. **(CM-IDAM.S4)** The service provider shall implement measures to adopt a **Zero Trust Model,** ensuring that all access to the organisation's resources by individuals, devices, and other resources is continuously verified and strictly controlled. 5. **(CM-IDAM.S5)** The service provider shall implement measures to ensure **access rights are periodically reviewed and documented**. They shall also use a **Maker-Checker framework** for granting, revoking, and modifying user rights in applications and databases, etc.

			6. **(CM-IDAM.S6)** The service provider shall implement measures for **documenting and implementing a comprehensive authentication policy**. This policy requires that **identities be proven, securely bound to credentials, and asserted during all interactions.** Authentication for **users, devices, and other assets** will utilize either single-factor or multifactor methods, with the chosen method **commensurate with the risk level of the operation (**including risks to individuals' security and privacy, and other organisational risks). 7. **(CM-IDAM.S7)** The service provider shall implement measures to ensure that all *critical systems* have **Multi-Factor Authentication (MFA)** implemented for all users accessing from either an untrusted network or trusted network.

			8. **(CM-IDAM.S8)** The service provider shall document and implement a comprehensive log management policy. 9. **(CM-IDAM.S9)** The service provider shall implement measures to ensure that user logs shall be uniquely identified and stored for a period in line with the provisions of the Cybercrime Act and the NCC subsidiary legislations. 10. **(CM-IDAM.S10)** The service provider shall implement measures to ensure that physical access to assets is managed, monitored, and protected. Physical access to the *critical systems* shall be monitored and recorded on a continuous basis. Some of the physical security controls include the following: a. Service providers shall document physical security-specific policies which include

			physical access control, monitoring, continuity of operations, (multi-vendor) spare part management etc b. Service providers shall ensure that individuals are screened before granting them access to the organisational information systems c. Service providers shall ensure the physical security of assets during transportation from one location to another d. Service providers shall ensure environmental controls such as fire, flood, and gas (FFG) and heating, ventilation, and air conditioning (HVAC) are interlinked with security management e. Service providers shall ensure that facilities maintenance reporting is interlinked with security management

			f. Service providers shall be required to conduct inspections and confirm the use of raceway/conduit for the protection of cables/fibre for facility and equipment g. Service providers shall ensure site access management controls are implemented h. Service providers shall ensure physical security standards and risk assessments are carried out depending on the class of sites (office environments, data centres, operations centres, remote sites (manned/unmanned/lights-out), public access) i. Service providers shall ensure multiple power supply continuity strategies are in place to avoid a single point of supply failure. 11. **(CM-IDAM.S11)** The service provider shall implement measures to ensure that

			privileged users' activities shall be periodically reviewed. Access restriction shall be implemented for employees as well as third-party service providers. If it is required to grant access, it shall be for the limited time- period, on need-to-know basis and shall be subject to stringent supervision and monitoring. 12. **(CM-IDAM.S12)** The service provider shall implement measures to ensure that remote access to assets shall be strictly tracked and administered. 13. **(CM-IDAM.S13)** The service provider shall implement measures to ensure that a comprehensive data-disposal and data-retention policy shall be documented and implemented and in compliance with relevant national laws and the Commission's subsidiary legislations.

			14. **(CM-IDAM.S14)** The service provider shall implement measures to ensure that comprehensive Standard Operating Procedures (SOPs) shall be documented for handling data storage and their disposal. 15. **(CM-IDAM.S15)** The service provider shall implement measures to ensure that access control for using systems such as endpoint devices, networks, APIs, removable media, laptops, mobiles, etc. shall be defined and implemented. 16. **(CM-IDAM.S16)** The service provider shall implement measures to ensure that mobile applications shall be properly vetted against security requirements, and thoroughly tested before deployment. 17. **(CM-IDAM.S17)** The service provider shall implement measures to ensure API security with proper authentication and

			authorisation mechanisms shall be defined and implemented.
	CM-NSG: Network Security (General)	This control objective is to protect the network and its resources from unauthorized access, misuse, disruption, or destruction. It aims to create a secure and trusted environment for data communication, storage, and processing, thereby protecting the service provider's	1. **(CM-NSG.S1)** The service provider shall deploy adequate controls to address various Indicators of Compromise (IOCs) on servers and other IT/OT systems. These controls may include host/network sensors, application-based IPs, customised kernels, and anti-malware software, Endpoint Security Solutions, Anti-virus definition, etc. 2. **(CM-NSG.S2)** The service provider shall establish information security policy and procedure documents to facilitate consistent application of security configurations to network operations. Service providers shall also conduct regular monitoring, and enforcement checks to ensure that these are uniformly applied.

		assets, reputation, and operations.	3. **(CM-NSG.S3)** The service providers shall define and implement relevant technical security requirements at the data, network and infrastructure levels covering 2G, 3G, 4G and 5G technologies across the Core Layer, the Transmission/IP Layer, access Layer, and the Management Plane. The service provider shall implement cybersecurity mechanisms on both IP protocols (IPv4 and IPv6) to protect the network through end-to-end encryption, authentication, and integrity checks for network traffic. 4. **(CM-NSG.S4)** The service provider shall develop an implementation plan towards migration to IPv6. 5. **(CM-NSG.S5)** Service providers shall develop plans to address the issues in migrating from IPv4 to IPv6, as well as

			configuration guidance, and provide adequate training to their network administrators. 6. **(CM-NSG.S6)** Service providers shall comply with relevant international standards related to network security.
	CM-NSCI: Network Security (Critical Infrastructure)	This control objective enables service providers to prepare for evolving threats by having a system aligned with a **Zero-Trust Architecture** (ZTA) that secures micro-perimeters across the entire mobile network and provides the ability	1. **(CM-NSCI.S1)** The service provider shall align with best practices, regulatory and industry standards and guidelines to ensure a secure approach to network security using ZTA. 2. **(CM-NSCI.S2)** The service provider shall ensure that vendors and third-party suppliers follow a secure service/product development process and implement required security functionality in line with the risk assessment framework of the service provider.

		to identify, protect, detect, respond, and recover from evolving attacks. **Specific objectives of this control include:** - The service provider shall treat each network function as a resource and secured as micro-perimeter - The service provider shall ensure that	3. **(CM-NSCI.S3)** The service provider shall define a security management function that bridges the security view across the following heterogenous network and IT elements – Cloud Infrastructure Solutions, Network Function Virtualisation Infrastructure (NFVI). It must also address security layers across Linux security, Container/Kubernetes Security, Telecom Application Security, Telecom Service Security. 4. **(CM-NSCI.S4)** The service provider shall have a security management function that enforces the security controls across all mobile network domains – Legacy OSS/BSS, 3G/4G Core IMS, Cloud OSS/BSS, 5G Core and beyond, Cloud RAN, RAN, Open RAN and transport and relates them in a security operations workflow.

		confidentiality and integrity protection (encryption) is provided for all data - The service provider shall enforce authentication and authorization on a per-session basis for external and internal subjects - The service provider shall	5. **(CM-NSCI.S4)** The security management function of the service provider must achieve strong data encryption and integrity checking, including key management protocols (data at rest and data in transit). 6. **(CM-NSCI.S6)** The service provider shall implement automated Identity access Management (IAM) with dynamic access control. 7. **(CM-NSCI.S7)** The service provider shall implement strong mutual authentication with PKIX. 8. **(CM-NSCI.S8)** The service provider shall implement user MFA. 9. **(CM-NSCI.S9)** The service provider shall implement micro segmentation, container isolation, and tenant isolation security techniques.

		ensure that continuous monitoring, logging, and alerting is implemented to detect and respond to security events	10. **(CM-NSCI.S10)** The service provider may implement ML/AI for anomalous behaviour detection with adequate considerations for the limitations of ML/AI. 11. **(CM-NSCI.S11)** The service provider shall implement a threat intelligence detection and response mechanism that allows management of vulnerabilities, sharing, and escalation of threat intelligence and events with sectoral and national supervising authorities (NCC-CSIRT). 12. **(CM-NSCI.S11)** The service provider shall define and automate the continuous monitoring, logging, and validation of robust security configuration functions using Machine Learning and Artificial Intelligence (AI) concepts.
	CM-PS: Personnel Security	This control objective aims to	1. **(CM-PS.S1)** The service provider shall establish measures to mitigate the risk of

		mitigate risks related to human actions, whether intentional or unintentional, that could compromise the service provider's security. Its purpose is to ensure that individuals with access to systems, data, and facilities are trustworthy and pose minimal risk to the organisation.	intentional malicious actions by personnel or other individuals with access to the data and systems in the service provider's environment. These measures include, but are not limited to, personnel screening, ongoing monitoring, and the application of sanctions where appropriate. 2. **(CM-PS.S2)** The service provider shall establish measures to mitigate the risk of intentional harm caused by personnel or other individuals who have access to the data and systems of the service provider. These measures include, but are not limited to, basic cyber-hygiene practices, proper network and IT/OT configuration, removable media control, license management control, and purge of dismissed devices.

	CM-ES: Endpoint Security	This control objective aims to safeguard devices (endpoints) and the data they access from cyber threats, ensuring the integrity, confidentiality, and availability of information. This includes implementing measures to prevent, detect, and respond to attacks targeting these devices, which serve as entry	1. **(CM-ES.S1)** The service provider shall deploy Solutions such as Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Managed Detection and Response (MDR), Next-Generation Intrusion Prevention System (NG-IPS), anti-malware software, and similar technologies to detect threats and attacks on endpoint devices and to facilitate immediate response. Additionally, service providers must ensure that threat signatures are regularly updated across all IT systems. 2. **(CM-ES.S2)** PowerShell and local administrative rights shall be disabled by default on endpoint machines and shall be used only for a specific purpose and for a limited time. 3. **(CM-ES.S3)** The service provider shall

		points to the broader network of the service provider.	implement DNSSEC, or other security measures aimed at enhancing the security of Domain Name Systems (DNS). 4. **(CM-ES.S4)** The service provider shall support DNSSEC initiatives and programmes at sectoral and national levels.
	CM-CH: Cyber Hygiene	Cybersecurity hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by service providers.	1. **(CM-CH.S1)** The service provider develops appropriate organisational and technical measures to identify and prioritise critical organisational services, products, and their supporting assets. 2. **(CM-CH.S2)** The service provider develops appropriate organisational and technical measures to identify, prioritise, and respond to risks to the organisation's key services and products. 3. **(CM-CH.S3)** The service provider shall develop appropriate organisational and technical measures to establish an incident

			response plan and report cyber incidents to the sectoral supervising authorities (NCC-CSIRT). 4. **(CM-CH.S4)** The service provider shall develop appropriate organisational and technical measures to conduct cybersecurity education and awareness activities. 5. **(CM-CH.S5)** The service provider shall develop appropriate organisational and technical measures to appoint the head of information security/cybersecurity in the organisation with responsibilities and authority for cybersecurity and shall report to the leadership of the organisation. 6. **(CM-CH.S6)** The service provider shall develop appropriate organisational and technical measures to comply with all relevant laws, regulations, and frameworks in the country and sector of their operation.

			7. **(CM-CH.S7)** The service provider shall develop appropriate organisational and technical measures to establish adequate network security and monitoring. 8. **(CM-CH.S8)** The service provider shall develop appropriate organisational and technical measures to control access based on least privilege and maintain the user access account consistent with the cybersecurity goal of the organisation. 9. **(CM-CH.S9)** The service provider shall develop appropriate organisational and technical measures to adapt to technology changes and use standardised secure configurations. 10. **(CM-CH.S10)** The service provider develops appropriate organisational and technical measures to implement controls to protect and recover data.

			11. **(CM-CH.S11)** The service provider develops appropriate organisational and technical measures to prevent and monitor malware exposures. 12. **(CM-CH.S12)** The service provider develops appropriate organisational and technical measures to manage cyber risks associated with suppliers and external dependencies. 13. **(CM-CH.S13)** The service provider develops appropriate organisational and technical measures to perform cyber threat and vulnerability monitoring and remediation. 14. **(CM-CH.S14)** The service provider develops appropriate organisational and technical measures to participate in cybersecurity stakeholders' activities to inform, collaborate, share, and advance cybersecurity services within the communications sector.

	CM-CIR: Communication Infrastructure Resilience	This control objective defines clear cyber resiliency strategic objectives and the need to incorporate these objectives into the service provider's risk management framework. This control objective enables service providers to prepare for evolving threats by having a system aligned with a **Zero-Trust Architecture** (ZTA)	1. **(CM-CIR.S1)** The service provider shall implement measures to continue the duration and viability of essential mission or business critical functions during adversity e.g. by ensuring the availability of services and minimizing the impact of service degradation. 2. **(CM-CIR.S2)** The service provider shall implement measures to limit damage from adversity e.g. by identifying and isolating compromised assets. 3. **(CM-CIR.S3)** The service provider shall implement measures to ensure the restoration of business functionality (in line with the RTO and RPO specified in the Service Provider's BCP) after an attack and determine the trustworthiness of restored resources. **4. (CM-CIR.S4)** The service provider shall

		that secures micro-perimeters across the entire mobile network and provides CI owners with the ability to identify, protect, detect, respond, and recover from evolving attacks. **Specific objectives of this control include:** - Identify critical infrastructure, analyze (inter-)dependencies, and prioritize essential	implement measures to align the organisation's cybersecurity resiliency strategy with industry best practices and standards. 5. **(CM-CIR.S5)** Service providers shall adopt an all-hazards and threats, forward-looking approach to critical infrastructure resilience and security. This approach allows regulator and service providers to better anticipate and prepare for unforeseen events. 6. **(CM-CIR.S6)** System-level: Service providers shall take a systems approach to enable the prioritization of the most critical components and helps identify and address vulnerabilities that could pose significant risks to the entire system. 7. **(CM-CIR.S7)** Service providers shall embrace cross-sector coordination programmes and ensure maximum cooperation with multi-

		services, functions, systems, and assets that require the most investment in resilience and security. - Establish strategic partnerships with critical infrastructure service providers to foster mutual trust, facilitate information	sectoral coordination initiatives including public-private collaborative partnerships. 8. **(CM-CIR.S8)** Service providers shall invest in design measures, such as robustness and redundancies, during the early phases of the infrastructure life cycle. Service providers shall focus on business continuity planning and maintenance during operations. Service providers shall establish a comprehensive policy that supports resilience throughout the entire infrastructure life cycle is essential. 9. **(CM-CIR.S9)**: Service providers shall develop and implement a comprehensive resilience policy encompassing measures across the entire risk management cycle, including risk assessment incorporating dependencies and criticality assessments, prevention,

		sharing on risks and vulnerabilities, and collaboratively develop a shared vision and policy objectives. - Share responsibilities for safeguarding critical infrastructure assets and ensuring rapid service restoration	emergency preparedness, response, recovery, and reconstruction. 10. **(CM-CIR.S10):** Service providers shall develop a risk-based and layered approach to effectively addresses these complexities, encompassing all hazards and considering the entire infrastructure life cycle. 11. **(CM-CIR.S11)**: Service providers shall support strong international cooperation and coordinated global efforts to enhance infrastructure resilience. 12. **(CM-CIR.S12)** IP Address Monitoring: All live Internet Protocol (IP) addresses issued by service providers must be logged and audited (biannually) to identify IPs that are used on CNII.

		- Ensure continuous monitoring, logging, and alerting to detect and respond to security events and attacks on critical infrastructure	
	CM-ED: External Dependencies/Supply Chain/Procurement	This control objective assesses whether service providers have considered cybersecurity risks associated with interconnections	1. **(CM-ED.S1)** The service provider's procurement processes include cybersecurity requirements for vendors and/or service providers (e.g., due diligence; third-party audit; certifications; notification of security incidents or vulnerabilities in their assets; etc).

		with other entities, both within and outside the sector, as well as the inherent vulnerabilities of networked systems like cloud technologies. It also evaluates the technical and organisational measures the service providers have implemented to mitigate these risks.	2. **(CM-ED.S2)** The service provider shall adopt measures to mitigate the risks related to the use of cloud technologies. 3. **(CM-ED.S3)** The service provider shall require ICT providers to be accredited/certified in cybersecurity before/if procuring hardware, software, digital services, etc. from those vendors. 4. **(CM-ED.S4)** The service provider shall implement cyber security hygiene expectations e.g. patching and following cyber supply chain risk management standard practices. 5. **(CM-ED.S5)** The service provider shall ensure that manufacturers of critical components should provide, for example, an ISO 28000 statement of compliance or local regulation compliance issued by NCC in its Type Approval Regulations 2024 and

			its subsisting Business Rules. 6. **(CM-ED.S6)** The service provider shall ensure that manufacturers of 2G and subsequent generations of network equipment provide, for example, an ISO 27001/2 statement of compliance. 7. **(CM-ED.S7)** The service provider shall ensure that manufacturers of 2G and subsequent generations of network equipment provide, for example, an ISO 22301 statement of compliance. 8. **(CM-ED.S8)** The service provider shall ensure MSPs, MSSPs comply with best practices and international standards for all services provided under the scope of the service agreement. 9. **(CM-ED.S9)** The service provider shall define procedures to identify and manage the risks associated with third-party access to the

			service provider's systems and data. 10. **(CM-ED.S10)** The service provider shall define security control requirements for internal staff and resources, including privileged access of suppliers. 11. **(CM-ED.S11)** The service provider shall define contract, and due diligence checks for prioritized suppliers based on a pre-procurement risk assessment. 12. **(CM-ED.S12)** The service provider shall ensure that breach notifications are provided by suppliers in a timely manner. 13. **(CM-ED.S13)** The service provider shall ensure that manufacturers support integrity verification technologies in their products/solutions, including signed software and firmware packages, and secure delivery mechanisms for hardware and software.

			14. **(CM-ED.S14)** Service providers shall define and implement a risk-based patch management (e.g., deployment) policy on endpoint devices.
	CM-MR: Maintenance & Repairs	This control objective ensures that maintenance and repairs of network and information system components are performed consistent with policies and procedures.	1. **(CM-MR.S1)** The service provider must ensure that all maintenance and repairs of its assets are carried out using approved and controlled tools, and that these activities are properly documented. 2. **(CM-MR.S2)** Remote maintenance of the service provider's assets shall be approved, logged, and performed in a way that prevents unauthorized access. 3. **(CM-MR.S3)** The service provider shall ensure that patches shall be identified and categorised based on the severity of the vulnerability. Critical patches shall be implemented as soon as it is available. Patches shall be tested in non-production

			environment before applying to production or live environments. 4. **(CM-MR.S4)** The service provider shall ensure that security patch policies should include minimal–maximal deployment time limits, alternative mitigation options (if they exist) and cost-benefit analysis. 5. **(CM-MR.S5)** The service provider shall establish hardware lifecycle policies. 6. **(CM-MR.S6)** The service provider shall continuously monitor and evaluate the organisation's compliance against set patch management policies.
PILLAR 4: CYBERSECURITY INCIDENCE MANAGEMENT AND RESILIENCE	**CIRMR-IRP: Incidence Response Plan**	This control objective is to ensure that Incident response plans and procedures are	1. **(CIRMR-IRP.S1)** The service provider shall develop and implement measures to protect the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g.,

CIRMR: Objective This control objective examines whether service providers have planned their approach to detect, respond to, and recover from cybersecurity incidents. The objective is to comprehend the preparedness of service providers to respond and recover in the event of		actively executed and maintained to ensure an effective response to detected or known cybersecurity incidents.	plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems as well as and de-activation (when an incident/emergency/disaster is resolved). 2. **(CIRMR-IRP.S2)** The service provider shall develop and implement an incident response plan that identifies the assets and business processes necessary to sustain minimum operations (given the service provider's RTO and RPO). 3. **(CIRMR-IRP.S3)** The service provider shall perform security assessment of live systems to test the overall strength of an organisation's defence (the technology, the processes, and the people) by simulating the

cybersecurity incidents.			objectives and actions of an attacker and update the plan when the need arises. 4. **(CIRMR-IRP.S4)** The service provider's incident response plan shall use playbooks and use-cases to test effectiveness of detection processes. 5. **(CIRMR-IRP.S5)** The service provider shall ensure that its OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems (when applicable). 6. **(CIRMR-IRP.S6)** The service provider shall implement a holistic protective monitoring approach that ensures that there is a proactive and consistent approach to detection of abnormal behaviour on networks and systems. 7. **(CIRMR-IRP.S7)** The service provider shall collect, manage, and analyse audit logs of

			events that could help detect, understand, or recover from an attack. 8. **(CIRMR-IRP.S8)** The service provider shall control the installation, spread, and execution of malicious code at multiple points in the network, while optimising the use of automation to enable rapid updating of defence, data gathering, and corrective action.
	CIRMR-CSM: Continuous Security Monitoring	The service provider's information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	1. **(CIRMR-CSM.S1)** The service provider shall establish (or contracts) a Cyber Security Operations Centre (C-SOC) which shall encompass (including but not limited to) monitoring the network, endpoints, physical environment, personnel activities, malicious code, unauthorized mobile code, third-party service provider activities, and surveillance of unauthorized personnel, devices, connections, and software. The Cyber

			Security Operations Centre (C-SOC) must operate twenty-four hours daily for seven days a week in every day of the three hundred and sixty-five or six days of every given year (24/7/365-6) to continuously monitor, prevent, predict, detect, investigate, and respond to cyber threats. 2. **(CIRMR-CSM.S2)** The service provider shall ensure that appropriate and automated continuous security monitoring mechanisms shall be established in C-SOC for the timely detection of anomalous or malicious activities. 3. **(CIRMR-CSM.S3)** The service provider shall ensure that all anomalies and alerts generated shall be properly monitored and investigated within the stipulated time as defined in the CRF-NCS.

			4. **(CIRMR-CSM.S4)** The service provider shall ensure that capacity utilisation is monitored for all the critical systems in the organisation. 5. **(CIRMR-CSM.S5)** The service provider shall ensure that cybersecurity audit, configuration audit, implementation audit, change management audit, and VAPT shall be conducted to detect vulnerabilities in IT and OT environments.
	CIRMR-DP: Detection Process	This control objective is to ensure that detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	1. **(CIRMR-DP.S1)** The service provider shall implement measures to ensure that event detection information is communicated in line with regulatory requirements contained in the CRF-NCS and organisational policies. 2. **(CIRMR-DP.S2)** Service providers shall conduct goal-based adversarial simulation red teaming exercises on a periodic basis to identify potential weaknesses within the organisation's cyber defense.

			3. **(CIRMR-DP.S3)** Service providers shall conduct threat hunting and compromise assessment on a regular basis.
	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan)	This control objective assesses the measures implemented by service providers to detect, respond to, and recover from cybersecurity incidents. The focus is on understanding whether service providers have established both technical and organisational measures to	1. **(CIRMR-CCMP.S1)** The service provider shall ensure the documentation of a comprehensive Cyber Crisis Management Plan ((CCMP) that includes scenario-based Standard Operating Procedures (SOP). The incident response management plan shall also be integrated into the (CCMP. Furthermore, the response plan and the execution of the necessary SOPs shall be promptly activated as soon as an incident occurs. 2. **(CIRMR-CCMP.S2)** Service providers shall enhance their capacity to respond promptly and effectively to adverse conditions, stresses, attacks, or Indicators of Compromise (IOC). This will help maximize

		manage incidents and crises, and whether these measures are regularly tested to evaluate their effectiveness. Additionally, it reviews whether service providers share knowledge and lessons learned from incident management to improve overall resilience of the sector.	their ability to maintain business operations, minimize impacts, and prevent destabilization. 3. **(CIRMR-CCMP.S3)** Service providers shall prepare contingency plans, training, exercises, and incident response and recovery plans for their systems and infrastructure and get them approved from their respective leadership. 4. **(CIRMR-CCMP.S4)** When an incident is detected, service providers shall ensure that there are dedicated personnel (e.g., Incident Response Team) tasked with analyzing (incident triage) and classifying the incident according to a pre-defined taxonomy and scenarios, and verifying what assets (e.g., information; applications; servers; etc.) have been compromised. Further, newly identified

			vulnerabilities shall be mitigated or documented as accepted risks. 5. **(CIRMR-CCMP.S5)** Service providers shall ensure that lessons learned from incident handling activities are incorporated into incident response plans, training, and testing, and resulting changes shall be implemented accordingly. Changes to the response plan shall be communicated to the service provider's designated key personnel. 6. **(CIRMR-CCMP.S6)** Service providers shall ensure that thorough investigations of cybersecurity incidents and alerts are conducted, including forensic analysis where appropriate. This process aims to identify the root cause of the incident, understand the threat actor's modus operandi, track any lateral movement of the threat actor, and

			implement measures to prevent similar incidents from recurring. 7. **(CIRMR-CCMP.S7)** The service provider shall conduct an impact analysis of the incident. Root Cause Analysis (RCA) and forensics analysis (as appropriate) shall be performed as per '*Classification and Handling of Cybersecurity Incidents*' SOP (Annexure IV). 8. **(CIRMR-CCMP.S8)** The service provider shall document and track cybersecurity events and incidents to closure. Internal stakeholders (e.g., executives, legal department, etc.) are identified and notified of incidents, and the response is coordinated accordingly. 9. **(CIRMR-CCMP.S9)** Service providers shall mandatorily get onboarded to the NCC-CSIRT's VTEM.

			10. **(CIRMR-CCMP.S10)** The service provider shall report cybersecurity breaches and incidents to NCC-CSIRT, in line with the provisions of this framework. 11. **(CIRMR-CCMP.S11)** The service provider may utilise Open-Source (threat) Intelligent (OSINT) platforms and other contextual information to increase awareness of the threat landscape.
	CIRMR-IRP: Incident Recovery Plan (Execution & Communication)	This control objective is to ensure that recovery processes and procedures are executed and maintained to ensure timely restoration of	1. **(CIRMR-IRP.S1)** The service provider shall maintain a recovery plan with different cyber-scenario-based classifications. 2. **(CIRMR-IRP.S2)** Recovery Time Objective (RTO) and Recovery Point Objective (RPO), specified by the Service Provider, shall be monitored for service restoration after a cybersecurity incident.

		systems or assets affected by cybersecurity incidents.	3. **(CIRMR-IRP.S3)** Service providers shall periodically conduct drills for testing different recovery scenarios. 4. **(CIRMR-IRP.S4)** The service provider shall ensure that backup and recovery plan of data is documented to ensure that there is no data loss. 5. **(CIRMR-IRP.S5)** The service provider shall define a public relations management in the recovery plan to manage external communication in the event of a cybersecurity incident. 6. **(CIRMR-IRP.S6)** Service providers shall communicate recovery activities to internal and external stakeholders as well as executive and management teams.
	CIRMR-RM: Resilience Management	This control objective seeks to adapt and improve	1. **(CIRMR-RM.S1)** Service providers shall develop strategies to anticipate new attack vectors by addressing identified

		the security posture to stay ahead of threats. It will help the business to recover and return to Business as Usual (BAU).	vulnerabilities or weaknesses through the addition or removal of controls. This includes reducing or adjusting attack surfaces and proactively adapting controls, practices, and capabilities to emerging, potential, or future threats. 2. **(CIRMR-RM.S2)** Service provider's architectures shall be designed to eliminate single points of failure with redundancy, cut-over management, and load-balancing. 3. **CIRMR-RM.S3)** Service provider shall enable capacity planning and management controls to prevent avoidable network outages. 4. **(CIRMR-RM.S4)** Service provider shall enable effective data backup and restoration processes (with regular tests of recovery). 5. **(CIRMR-RM.S5)** Service providers shall periodically exercise a service-specific

			documented Business Continuity Management (BCM) process. 6. **(CIRMR-RM.S6)** Service provider's cyber resilience capabilities shall be upgraded through periodic drills to ensure safe and timely restoration of critical operations. 7. **(CIRMR-RM.S7)** Service providers shall demonstrate heterogeneity to minimise common mode failures, particularly threat events exploiting common vulnerabilities. 8. **(CIRMR-RM.S8)** Service providers shall confirm post-incident modification of business functions and supporting processes to handle adversity and address environmental changes more effectively. In case of a cybersecurity incident, learning shall be incorporated to improve and evolve their cyber resilience posture.

			9. **(CIRMR-RM.S9)** Service providers shall continuously adapt and evolve to counter new cybersecurity threats and challenges using automated threat and exposure management systems.
PILLAR 5: CYBERSECURITY CAPACITY BUILDING AND DEVELOPMENT **Objective** This control objective assesses whether service providers are aware of the skills and capabilities required	**(CCB-CSD: Cybersecurity Skill Development**	The goal of cybersecurity skill development is to empower individuals (service provider and regulator staff as well as customers) with the knowledge and skills necessary to safeguard digital assets, reduce risks, and respond	1. **(CCB-CSD.S1)** The service providers shall regularly according to service provider's training plan) carry out training and education initiatives to make sure that all personnel are aligned with the cybersecurity skills and knowledge required by their distinct roles. Such training programs shall be conducted on a periodic basis and shall be updated as per emergence of new threats, state-of-the-art technologies and industry trends.

to achieve and sustain higher levels of cybersecurity maturity. It also evaluates the technical and organisational measures in place to develop and enhance these skills and capacities. Additionally, it reviews the initiatives and actions taken by service providers to promote cybersecurity		effectively to cyber threats. This encompasses understanding core cybersecurity principles, implementing appropriate security measures, and fostering a culture of security awareness within organisations.	2. **(CCB-CSD.S2)** The service providers shall ensure that privileged users understand their roles and responsibilities. 3. **(CCB-CSD.S3)** The service provider shall ensure that third-party stakeholders (e.g., suppliers, customers/investors, partners) understand their roles and responsibilities within the organisation's security framework. 4. **(CCB-CSD.S4)** The service providers shall ensure that physical and information security personnel understand their roles and responsibilities.

awareness across all organisational levels, from operational personnel to senior management.			
	(CCB-CTA: Cybersecurity Training and Awareness	This control objectives aim to reduce human error in security breaches, educate individuals about cyber threats, and foster a security-conscious culture within an organisation.	1. **(CCB-CTA.S1)** The service providers shall regularly carry out cybersecurity awareness activities, and new employees must receive initial cybersecurity training during their onboarding. 2. **(CCB-CTA.S2)** The service providers shall ensure that senior executives/ Board members understand their roles and responsibilities. Further, a dedicated program on cybersecurity, cyber resilience, and system hygiene shall be mandatorily conducted for Board members.

			3. **(CCB-CTA.S3)** The service providers shall develop a plan of action (with dedicated resources allocated) for cybersecurity advocacy in plain language for the users of communication services. This plan of action must be approved by the Board/Management of the service provider.
	(CCB-CRD: Cybersecurity Research & Development	This control objective adopts a multidisciplinary approach to strengthen the security and resilience of digital systems and data. It focuses on proactively identifying and addressing	1. **(CCB-CRD.S1)** The service provider should support and incentivize cybersecurity research and development and the dissemination of cybersecurity innovation in Nigeria's tertiary institutions. 2. **(CCB-CRD.S2)** The service provider should be encouraged to participate in Student Industrial Work Experience Scheme (SIWES) programmes for students in cybersecurity-related disciplines from Nigerian tertiary institutions.

		vulnerabilities, developing innovative defense mechanisms, and deepening our understanding of cyber threats.	
	(CCB-CE(CC: Cybersecurity Ecosystem and Cross-Sector Cooperation	This control objective examines whether the service providers promote or take part in initiatives aimed at fostering collaborative Partnership and in cybersecurity, both within and outside of the sector.	1. **(CCB-CECC.S1)** Service providers are encouraged to take part in Public Private Partnership initiatives that support and improve the cybersecurity posture of the communications sector, at national, regional and global levels. 2. **(CCB-CECC.S2)** Service providers are encouraged to take part in initiatives to strengthen the sectoral cybersecurity ecosystem. 3. **(CCB-CECC.S3)** Service providers are encouraged to take advantage of market

			levers and incentives offered at the national- or sectoral-level to implement/adopt cybersecurity standards and good practices.

ANNEXURE XII

SAMPLE CYBER ATTACK SCENARIO TEMPLATE FOR RISK MANAGEMENT TESTING

1. Scenario Title

(Provide a short, descriptive title, e.g., "Phishing-Induced Data Breach at ISP")

2. Scenario Description

Narrate the event timeline: how the attack started, method of compromise, systems affected, progression, and potential impact.

3. Attack Type and Vector

Attack Type	(e.g., Ransomware, Phishing, Insider Threat, DDoS, Supply Chain Attack)
Initial Attack Vector	(e.g., Malicious Email, Unpatched Server, Compromised Credentials)
Exploited Vulnerability	(e.g., Outdated software, Human error, Weak password policy)

4. Affected Assets/Systems

Asset/System	Type	Sensitivity	Impact

5. Potential Business Impact

- Data loss or leakage
- Financial loss
- Regulatory penalties
- Reputational damage
- Service disruption

6. Detection and Monitoring Mechanisms

Detection Method	Available (Yes/No)	Effectiveness

7. Response Strategy (Expected Actions)

- Activate Incident Response Plan
- Isolate affected systems
- Notify NCC/ngCERT
- Conduct forensic analysis
- Communicate with stakeholders
- Initiate recovery and containment

8. Mitigation & Recommendations

- Implement MFA
- Conduct phishing awareness training
- Patch vulnerable systems
- Review access controls
- Update firewall and antivirus signatures

9. Lessons Learned (Post-Simulation)

To be filled after the test: What went well? What failed? Where are the response gaps?

10. Simulation Type

Tabletop Exercise	Scenario-based discussion with key personnel
Live Simulation	Simulated technical attacks in a controlled environment
Red Teaming	External ethical attack to test defenses
Blue Team Response	Internal team defending in real-time

ANNEXURE XIII

1.0 Baseline Security Requirements

The baseline security requirements are categorized by the tier of the service providers. The table below depicts the categorization.

1.1 Baseline Requirements – All Service Providers

	CYBERSECURITY PROCESS/ACTIVITY	COMPLIANCE ARTEFACT
1	The service provider shall identify and prioritise critical organisational services, products, and their supporting assets	Approved list of critical assets, services, or functions
2	The service provider shall identify, prioritise, and respond to risks to the organisation's key services and products	Risk Management Framework
3	The service provider shall establish an incident response plan and mandatorily report cyber incidents to the sectoral supervising authorities (NCC-CSIRT and ngCERT).	Incident Management Framework
4	The service provider shall conduct cybersecurity education and awareness activities for the management and staff of the organisation.	Cybersecurity training plan
5	The service provider shall appoint the head of information security/cybersecurity in the organisation with responsibilities and authority for cybersecurity	Organisational chart with responsibilities and authorities of CISO
6	The service provider shall comply with all relevant laws, regulations, and frameworks in the country	Compliance statement
7	The service provider shall establish adequate network security and monitoring	Cybersecurity framework
8	The service provider shall control access based on least privilege and maintain the user access	Cybersecurity framework

	accounts consistent with the cybersecurity goal of the organisation	
9	The service provider shall manage technology changes and use standardised secure configurations including patching and following cyber supply chain risk management standard practices	Cybersecurity framework
10	The service provider shall implement controls to protect and recover data	Cybersecurity framework
11	The service provider shall prevent and monitor malware exposures	Cybersecurity framework
12	The service provider shall manage cyber risks associated with suppliers and external dependencies	Cybersecurity framework
13	The service provider shall perform cyber threat and vulnerability monitoring and remediation	Cyber drill reports
14	The service provider shall participate in cybersecurity stakeholders' activities to inform, collaborate, share, and advance cybersecurity services within the communications sector	Compliance evidence

1.2 Baseline Requirements – Tier 2

Tier 2 service providers are required to comply with baseline requirements for all service providers in addition to the following requirements.

	CYBERSECURITY PROCESS/ACTIVITY	COMPLIANCE ARTEFACT
1	**Board Level Engagement:** Service providers shall prioritize security at the Board level to prevent gaps in understanding of risk posture, priorities, and cybersecurity investments. This disconnect can introduce unnecessary security and fraud risks, undermining the service provider's resilience and trustworthiness	Minutes of Board or Board committee meetings
2	**Appointment of CISO:** Service providers shall establish a formal role that recognizes security as a key responsibility, often fulfilled by the	Organisational chart with responsibilities

	CISO. Alternatively, this role can be held by any senior individual whose position enables them to influence and direct enterprise-wide investment and strategic changes	and authorities of CISO
3	**Organisational Policy:** Service providers shall implement approved organizational policies as a collection of rules that the organization is expected to follow. Specific policies related to security should align with the organization's overall security strategy and principles, serving as a foundation that supports and reinforces its security objectives	Approved policies
4	**Governance, Risk Management, and Compliance (GRC:** Service providers shall align their governance with organizational policies, while reporting is shared with senior leadership to demonstrate the overall success of the security program. Additionally, service providers shall ensure that all projects should undergo security assessments to ensure they are designed with security in mind from the outset.	Cybersecurity & Resilience Framework
5	**Data protection and privacy assessment**.: Service providers shall ensure that all projects undergo a data protection and privacy assessment. This assessment must align with local policies, industry regulations, and applicable legislation, which will collectively guide the principles for local data management	Data Magement Policy and/or Cybersecurity Framework
6	**A Secure Software Development Life Cycle (SDLC):** Service providers shall implement SDLC, incorporating quality control stages that include code reviews at both module and system levels. This process should involve static and dynamic testing to ensure security. Additionally, the choice of programming language should consider security considerations, such as type safety and the avoidance of vulnerable functions	Cybersecurity & Resilience Framework

7	**Business Continuity Management (BCM):** Service providers shall enhance their resilience by building the capacity to detect, prevent, minimize, and respond to disruptive events. In the event of an incident, the BCM plan ensures that critical activities can continue smoothly. Over the longer term, it supports the organization's recovery efforts and helps return operations to Business as Usual (BAU).	BCM/DRP and/or Cybersecurity & Resilience Framework
8	**Physical Security Controls**. Service providers shall minimize the risk of a physical attack, enabling a subsequent logical attack. A service provider's security strategy should take a comprehensive and integrated approach to physical security controls and procedures.	Cybersecurity & Resilience Framework
9	**Supply Chain and Procurement Controls:** Service providers shall establish robust supply chain and procurement controls to ensure that the services they deliver and operate adhere to legal requirements and address supply chain threats. Additionally, they should implement controls for third-party access and outsourcing to effectively manage the risks associated with information sharing and external service provision	Supply Chain Management Policy and/or Cybersecurity & Resilience Framework
10	**Decommissioning of Equipment** : Service providers shall have a decommissioning programme to ensure that equipment reaching End of Life (EoL) are systematically removed from the infrastructure. In addition, the decommissioning of equipment should include secure sanitization or disposal procedures to prevent the risk of data leaks following the equipment's decommissioning	Cybersecurity & Resilience Framework
11	**Infrastructure Protection:** Hardware and software products should be safeguarded against tampering, whether through supply chain poisoning or by internal threat agents with privileged access	Cybersecurity & Resilience Framework

12	**International Standards:** Service providers shall align their cybersecurity practices and compliance efforts with internationally recognized standards and cybersecurity frameworks.	Relevant international certifications
13	**Cyber Resilience:** Service providers shall establish clear strategic objectives for cyber resilience and integrate these objectives into the organization's overall risk management framework	Cybersecurity & Resilience Framework

1.3 Baseline Requirements – Tier 1

Tier 1 service providers must adhere to the baseline requirements applicable to all service providers, the baseline requirements for Tier 2, and the additional specific requirements outlined below:

	CYBERSECURITY PROCESS/ACTIVITY	COMPLIANCE ARTEFACT
1	**Authentication and Authorization:** Service providers shall implement secure authentication and authorization protocols to regulate access to network equipment and services	Network Security Policy
2	**Encryption:** Service providers shall utilize (robust cryptographic security) encryption methods, such as AES and IPsec, to safeguard data during transmission, storage, and processing.	Data Protection Policy
3	**Firewalls and Access Controls:** Service providers shall deploy firewalls and access controls, such as ACLs and VLANs, to prevent unauthorized access to network equipment and services.	Network Security Policy
4	**Intrusion Detection and Prevention:** Service providers shall implement intrusion detection and prevention systems (IDPS) to identify and block unauthorized access and malicious activities.	IDS and IPS subscriptions

5	**Regular Security Audits and Penetration Testing:** Service providers shall conduct regular security audits, vulnerability assessments, and penetration testing to identify and address security weaknesses.	Up-to-date VAPT Report
6	**Security Information and Event Management (SIEM):** Service providers shall deploy a SIEM system to gather, monitor, and analyze security-related data from multiple sources.	SIEM subscription and up-to-date log
7	**Compliance with Regulatory Requirements:** Service providers shall ensure compliance with relevant regulatory requirements and national laws	Compliance certifications

1.4 Baseline Requirements – MNOs

MNO service providers must comply with the baseline requirements for all service providers, as well as the specific baseline requirements for Tiers 1 and 2, along with the additional network configuration requirements outlined below:

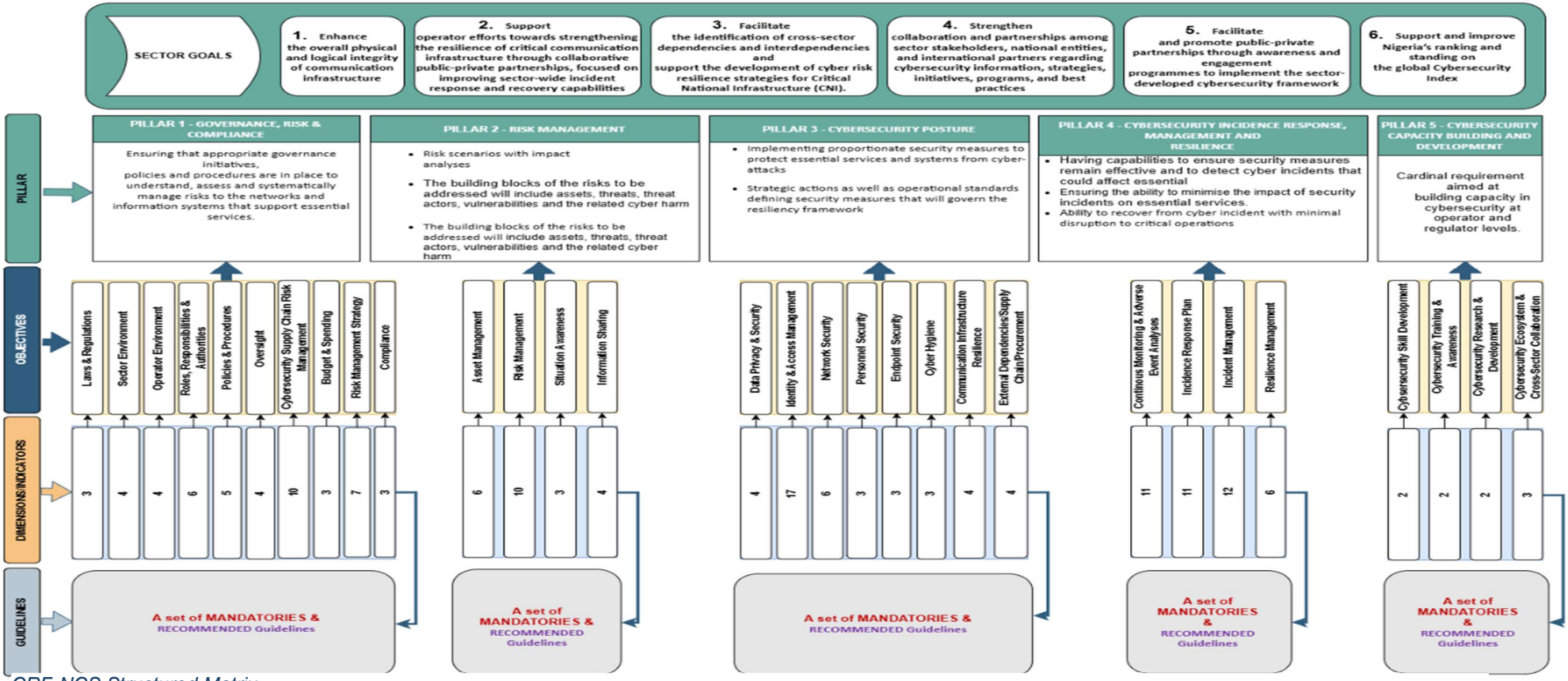
	CYBERSECURITY PROCESS/ACTIVITY	COMPLIANCE ARTEFACT
1	**Transmission Network:** - Service provider shall implement secure transmission protocols (e.g., SDH, SONET) to prevent unauthorized access and data tampering. - Service provider shall use encryption to protect transmitted data. 2. IP/MPLS Network: - Service provider shall implement secure IP routing protocols (e.g., OSPF, BGP) to prevent unauthorized access and routing table modifications. - Service provider shall use robust cryptographic security encryption (e.g., IPsec) to protect IP/MPLS data.	Network Security policy

	3. Network Devices: - Service provider shall implement secure device management protocols (e.g., SSH, SNMPv3) to prevent unauthorized access and device configuration modifications.	
2	**Access Layer** 1. Radio Access Network (RAN): - Service provider shall implement secure radio access protocols (e.g., LTE, UMTS) to prevent unauthorized access and data tampering. - Service provider shall use encryption to protect RAN data. 2. Base Transceiver Stations (BTS): - Service provider shall implement physical security measures (e.g., access controls, surveillance) to protect BTS equipment. - Service provider shall use secure authentication and authorization mechanisms to control access to BTS equipment.	Network Security policy
3	**Management Plane** 1. Configuration Management: - Service provider shall implement secure configuration management protocols (e.g., NETCONF, RESTCONF) to prevent unauthorized access and configuration modifications. - Service provider shall use encryption (e.g., SSL/TLS) to protect configuration data. 2. Monitoring and Management: - Service provider shall implement secure monitoring and management protocols (e.g., SNMPv3, Syslog) to prevent unauthorized access and monitoring data modifications. - Service provider shall use encryption (e.g., SSL/TLS) to protect, monitor and manage data.	Network Security policy

4	Service provider shall implement DNS Security Extensions (DNSSEC).	Network Security policy

ANNEXURE XIV

CRF-NCS STRUCTURED MATRIX



CRF-NCS Structured Matrix