



GUIDANCE NOTE: IMPLEMENTATION OF CYBER RESILIENCE FRAMEWORK FOR THE NIGERIAN COMMUNICATION SECTOR (CRF- NCS)

July 2026

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
Tier 3: Support service providers to other communication service providers				
Cyber Risk Management (CRM)				
CRM-AR.S1, CRM-AR.S2, CRM-AR.S4, CRM-AR.S5, CRM-AR.S6, CRM-AR.S7, CRM-SAIS.S1	CRM-AR – Asset and Risk Management; CRM-SAIS – Situation Awareness and Information Sharing	[B] 1. The Service Provider shall keep an up-to-date inventory of their hardware and systems, software, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets), interfacing systems (both internal and external), network resources, network connections, encryption methods, and data flows. [B] 2. Any additions, deletions, or modifications to existing assets shall be updated in the asset inventory within three working days. [B] 3. To conduct the criticality assessment of assets, Service Providers shall undertake the following steps (including, but not limited to): [B] a. Maintain a comprehensive asset inventory [I] b. Conduct threat modelling (based on risk assessment) [B] c. Conduct a vulnerability assessment	Approved IT asset inventory that is up to date	TIER 3
GC-RM.S1, GC-RM.S2,	GC-RM – Risk Management Strategy;	[B] The Service providers shall identify, prioritise, and respond to risks to the organisation's key services and products by:	Risk Management Framework Outcome of	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
GC-RM.S3, GC-RM.S4, GC-RM.S5, CRM-RA.S1, CRM-RA.S5, CRM-RA.S6, CRM-RA.S7, GC-RRA.S7	GC-RRA – Roles, Responsibilities & Authorities; CRM-RA – Risk Assessment	• Risk Management Activities including, but not limited to 1. Identification of the cybersecurity risk for the organisation 2. Classification of identified and mapped business functions, supporting processes and information assets at risk. 3. Determination of risk appetite for IT and cybersecurity risks. 4. Definition of mitigation measures and controls to reduce the risks. 5. Monitoring of the effectiveness of the above-mentioned measures and controls. 6. Evaluation of the effect of major changes and significant operational, technical or cybersecurity incident(s) on the risks. • Service Providers shall periodically evaluate the level of employee cybersecurity awareness, for example, by measuring metrics such as phishing test success rates, Business Email Compromise (BEC) success rate, among other indicators	risk assessment and evaluation activities	TIER 3
CIRMIR-IRP.S1; CIRMIR-IRP.S2; CIRMIR-CCMP.S1; CIRMIR-CCMP.S6; CIRMIR-CCMP.S7; CIRMIR-CCMP.S8; CIRMIR-CCMP.S9; CIRMIR-CMP.S10; CRM-SAIS.S6; CRM-SAIS.S7; CM-CH.S3	CIRMIR-IRP (Incident Response Plan); CIRMIR-CCMP (Cyber Crisis Management Plan); CRM-SAIS (Situation Awareness/Info Sharing); CM-CH (Cyber Hygiene)	[B] The Service providers shall establish an incident response plan and mandatorily report cyber incidents to the sectoral supervising authorities (NCC-CSIRT). 1. All Service Providers shall develop an Incident Management Plan as part of their Cybersecurity Crisis Management Plan 2. The Incident Management plan shall outline the responsibilities and actions to be undertaken by employees and support or outsourced staff in the event of a cyberattack or cybersecurity incident. 3. All cyber-attack, cybersecurity incidents, and/or breach involving a Service Provider's system, network, or critical asset shall be reported to NCC-CSIRT within 4 hours of detection or awareness of the incident.	Incident Management Framework	

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
		This information shall be shared with NCC-CSIRT via incident@csirt.ncc.gov.ng within the same 4-hour timeline. Additionally, comprehensive details of the incident must be submitted through the NCC-CSIRT Incident Reporting Portal within 24 hours 4. Quarterly reports detailing cyber-attacks, threats, cybersecurity incidents, breaches experienced by Service Providers, and the measures taken to mitigate vulnerabilities, threats, and attacks—including information on bugs, vulnerabilities, and emerging threats that may be useful to other Service Providers and NCC—shall be submitted to NCC-CSIRT within 15 days after the end of each quarter (June, September, December, and March). 5. Such information, considered useful for sharing with other Service Providers in an anonymized or masked form, shall be shared using the mechanisms specified by NCC-CSIRT from time to time. When sharing the sensitive information, the Traffic Light Protocol (TLP) shall be used to indicate four levels of sensitivity: white, green, amber, or red. 6. During the incident investigation process by NCC-CSIRT, Service Providers shall, when necessary, provide regular updates, including reports such as Root Cause Analysis (RCA), forensic analysis reports, and other relevant progress reports on the ongoing incident analysis.		
CCB-CTA.S1; CCB-CTA.S2; CCB-CTA.S3; GC-RRR.S7; CM-CH.S4;	CCB-CTA (Cybersecurity Training & Awareness);	[B] The Service providers shall conduct cybersecurity education and awareness activities for the management and staff of the organization by: [B] 1. The Service Providers shall work on building awareness of cybersecurity, cyber resilience, and system hygiene among employees (with a focus on new employees, which should be part of their onboarding	Cybersecurity training plan Outcome of trainings and awareness programmes	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
CCB-CSD.S1	GC-RRA (Roles, Responsibilities & Authorities); CM-CH (Cyber Hygiene); CCB-CSD (Skill Development)	process). [B] 2. The Service Providers shall develop a dedicated program on cybersecurity governance responsibilities, building awareness of cybersecurity, cyber resilience, and system hygiene for board members and senior executives. The periodicity shall be bi-annual. [B] 3. The Service Providers shall focus on fostering awareness of cybersecurity, cyber resilience, and system hygiene for all employees, particularly emphasizing those in non-technical roles. The periodicity shall be bi-annual.		
GC-RRA.S3; GC-RRA.S4; GC-RRA.S5; CM-CH.S5; GC-LR.S5; GC-BS.S1; GC-BS.S2; GC-BS.S3; GC-BS.S4	GC-RRA (Roles, Responsibilities & Authorities); CM-CH (Cyber Hygiene); GC-LR (Laws & Regulations); GC-BS (Budget & Spending)	[B] The Service providers shall appoint the head of information security/cybersecurity or focal person in the organisation with responsibilities and authority for cybersecurity: [B] 1. Service Providers shall appoint a senior official or management personnel (hereafter referred to as the “Designated Officer”) responsible for assessing, identifying, and mitigating cybersecurity risks, responding to incidents, establishing appropriate standards and controls, and overseeing the development and execution of processes and procedures in accordance with the cybersecurity and cyber resilience policy or framework approved by the Board, Partners, or Proprietor. [B] 2. Service Providers shall establish a reporting procedure to ensure the timely communication of cybersecurity incidents or unusual activities within the organization to the Designated Officer, in accordance with the timeframes specified by the NCC's guidelines, policies, laws, circulars, frameworks, or other relevant directives. [B] 3. Service Providers designated as Critical National Information	Organisational chart with responsibilities and authorities of CISO/Focal person Acknowledgement of receipt of notification on appointment of CISO/Focal person	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
		Infrastructure (CNII) owners or Service Providers in accordance with the Official Gazette on the Designation and Protection of CNII Order, 2024, shall define the roles and responsibilities of the designated officer in alignment with the guidelines outlined in the same Official Gazette. [B] 4. NCC must be notified of the appointment of the Designated Officer and their Job Description in writing (letter and/or email), and acknowledgment must be made available for compliance and audit verifications. [B] 5. Service Providers shall allocate an appropriate percentage of the total company budget to cybersecurity. This allocation shall be designated under a separate budgetary category to facilitate monitoring and oversight by the Board of Directors and top-level management. [B] 6. Service Providers shall ensure that sufficient resources are allocated and aligned with the cybersecurity risk strategy, roles, responsibilities, and policies. These resources should be specified in terms of budget, personnel, and materials. Resourcing needs shall be reviewed regularly, based on the progress or gaps in implementing cybersecurity standards, and any updates shall be reflected in the budgetary allocations.		
GC-LR.S1; GC-LR.S2; GC-LR.S3; GC-LR.S4; GC-LR.S5; GC-C.S1; GC-C.S2;	GC-LR (Laws & Regulations); GC-C (Compliance); CM-DP (Data Privacy); CM-IDAM (Identity & Access Mgmt);	[B] The Service providers shall comply with all relevant laws, regulations, and frameworks in the country by: [B] 1. Service Providers shall retain appropriate logs, user IDs, and traffic data in-country for at least 2 years. Service Providers shall provide access to law enforcement with a warrant. [B] 2. Service Providers shall notify the ngCERT and the NCC-CSIRT of significant system breaches within the time stipulated in this framework	Evidence of Compliance	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
GC-C.S3; GC-C.S4; CM-DP.S3; CM-DP.S4; CM-IDAM.S9; CM-CH.S6	CM-CH (Cyber Hygiene)	and using the template provided in Annexure I [B] 3. Service Providers shall demonstrate the implementation of systems to prevent network use for cybercrime (e.g., fraud, hate speech) and cooperate with investigations [B] 4. Service Providers shall demonstrate implementation of secure infrastructure against unlawful interference [B] 5. Service Providers shall comply with the NDPA Act (2023) [B] 6. The Service Provider shall comply with all relevant provisions of the NCC Comprehensive Cybersecurity Framework and shall demonstrate evidence of on-going compliance through self-assessment [B] 7. Service Providers shall comply with all communications sector regulatory instruments; relevant Executive Orders and applicable national frameworks. [B] 8. The Service Provider shall comply with all relevant laws of the Federal Republic of Nigeria [B] 9. Service Providers are encouraged to comply with relevant international cybersecurity standards and frameworks		
CM-NSG.S1; CM-NSG.S2; CM-CH.S7; CM-ES.S1	CM-NSG (Network Security – General); CM-CH (Cyber Hygiene); CM-ES (Endpoint Security)	[B] The Service providers shall establish adequate network security and monitoring: [B] 1. Service Providers shall ensure the implementation of appropriate controls to protect against viruses, malware, and ransomware attacks on servers and other IT systems. These may include host-, network-, and application-based intrusion prevention systems (IPS), customized Linux kernels, and antivirus and antimalware software, among other security measures. Furthermore, updates to anti-virus definition files and automatic	Cybersecurity framework And/or Network security policy	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
CM-IDAM.S1; CM-IDAM.S3; CM-IDAM.S5; CM-IDAM.S6; CM-IDAM.S7; CM-IDAM.S9; CM-IDAM.S11; CM-IDAM.S12; CM-IDAM.S13; CM-CH.S8	CM-IDAM (Identity & Access Management); CM-CH (Cyber Hygiene)	system scans shall be conducted regularly to ensure ongoing system security [B] The Service providers shall control access based on least privilege and maintain the user access accounts consistent with the cybersecurity goal of the organization by [B] 1. No individual, regardless of rank or position, shall have an inherent right to access confidential data, applications, system resources, or facilities. Access shall be granted strictly based on defined roles, responsibilities, and approved authorization protocols. [B] 1. Access to Service Providers' systems, applications, networks, databases, and other resources shall be granted only for a specified purpose and a defined period. Access to IT systems, applications, databases, and networks shall be on a need-to-know basis, adhering to the principle of least privilege. Such access shall be provided for a limited duration and secured through robust authentication mechanisms. [B] 2. User access rights, delegated access, unused tokens, and the activities of privileged users shall be reviewed regularly on a periodic basis. [B] 3. Access to external cloud services—such as Dropbox, Google Drive, iCloud, OneDrive, and similar platforms—shall be governed by the Service Provider's defined policy and granted only in accordance with approved guidelines [B] 4. Service Providers shall ensure that user access to critical systems is uniquely identifiable and properly logged whenever feasible, to facilitate auditing and review. These logs shall be securely stored for a minimum of two (2) years. Additionally, Service Providers must keep records of users	Cybersecurity framework, Access Control policy	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
		accessing shared accounts. [B] 5. Service Providers shall implement account access lock policies after failure attempts [B] 6. Service Providers shall ensure that regular reviews of existing user accounts and access rights are conducted to identify dormant accounts, accounts with excessive privileges, unknown accounts, or any discrepancies. [B] 7. Service Providers shall ensure that appropriate 'end of life' procedures are implemented for user management, including deactivating access privileges for users leaving the organization or whose access has been revoked. This applies to named user IDs, default user IDs, and generic email IDs. [B] 8. Service Providers shall ensure that all critical systems accessible via the internet are protected with multi-factor security measures, such as VPNs, firewall controls, and multi-factor authentication (MFA). [B] 9. Service Providers shall ensure that multi-factor authentication (MFA) is enabled for all users and systems accessing via online or internet connectivity, with particular emphasis on VPNs, webmail, and accounts that access critical systems from non-trusted environments to trusted environments.		
CM-MR.S3; CM-MR.S4; CM-MR.S5; CM-MR.S6; CM-DS.S5;	CM-MR (Maintenance & Repairs); CM-DS (Data Security);	[B] 1. The Service providers shall manage technology changes and use standardised secure configurations including patching and following cyber supply chain risk management standard practices. [B] 2. Service Providers shall develop and ensure that patch management procedures encompass the identification, categorization, and	Cybersecurity framework, Change Management Policy, Patch Management Policy	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
CM-CH.S9	CM-CH (Cyber Hygiene)	prioritization of patches and updates. Additionally, a specific timeframe for implementing each category of patches shall be established to ensure timely application. [B] 3. Service Providers shall ensure that all operating systems and applications shall be regularly updated with the latest patches. [F] 4. As an interim measure for zero-day vulnerabilities, and when patches are not immediately available, the service provider may implement virtual patching to protect systems (including legacy systems) and networks. This approach helps prevent cybercriminals from exploiting vulnerabilities in end-of-support or end-of-life applications and software. Patches must be obtained exclusively from the official sites of the Original Equipment Manufacturer (OEM). Additionally, the reasons and constraints necessitating virtual patching must be legitimate and properly documented. [B] 5. Service Providers shall ensure that all patches shall be first tested in a non-production environment that replicates the production environment. [I] 6. Service Providers shall ensure that hardware and software for critical systems shall be replaced prior to reaching their End-of-Life or End-of-Support status. [B] 7. Service Providers shall ensure that the procurement of hardware/software shall be aligned with their technology refresh policy. [B] 8. Service Providers shall develop a patch management policy to ensure that all relevant patches are identified, assessed, tested, and applied to all IT systems and applications in a timely manner. This policy shall be		

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
		approved by the IT Committee or leadership of the Service Providers. Furthermore, the IT Committee/leadership shall review the patch management policy at least once every year to ensure its continued effectiveness. [B] 9. Service Providers shall establish processes for monitoring patch compliance across all IT systems and applications and regularly report these findings to their respective IT Committee on a quarterly basis.		
CM-DS.S1; CM-DS.S4; CM-DP.S2; CM-IDAM.S15; CM-CH.S10	CM-DS (Data Security); CM-DP (Data Privacy); CM-IDAM (Identity & Access Mgmt); CM-CH (Cyber Hygiene)	[B] The Service providers shall implement controls to protect and recover data: [F] 1. Data shall be protected through strong encryption methods during transmission (in motion), storage (at rest), and processing (in-use). For data in use, encryption shall be applied in cloud deployments (refer to Annexure-VIII). Wherever feasible, a layered approach combining Full-Disk Encryption (FDE) with File-Based Encryption (FBE) shall be adopted. Service Providers shall utilize industry-standard, robust encryption algorithms such as RSA, AES, quantum encryption etc., whenever encryption is implemented. Illustrative measures related to this are provided in Annexure-VI and Annexure-VII. [F] 2. Service Providers shall implement measures to prevent unauthorized access, copying, or transmission of data and information held in a contractual or fiduciary capacity. It must be ensured that the confidentiality of information is maintained during the exchange and transfer of data with external parties. Illustrative measures to ensure security during data transmission over the internet are provided in Annexure-VII.	Cybersecurity framework ISO 27001 certifications	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
		[B] 3. Service Providers' information security policies shall also address the use of devices such as mobile phones, photocopiers, scanners, and other equipment that can be used to capture and transmit sensitive data within their IT infrastructure. This includes establishing access policies for personnel and defining network connectivity controls for these devices. [B] 4. To maintain data security, Service Providers shall validate and authorize all data storage devices before they are used within the IT infrastructure. [B] 5. Service Provider are encouraged to have relevant information security management standards such as ISO 27001		
CM-ES.S1; CIRMR-IRP.S7; CM-CH.S11	CM-ES (Endpoint Security); CIRMR-IRP (Incident Response Plan); CM-CH (Cyber Hygiene)	[B] 1. The Service providers shall prevent and monitor malware exposures. [I] 1. Service Providers shall deploy solutions such as EPP, EDR, XDR, and anti-malware software to detect threats and attacks on endpoint devices and facilitate rapid response. Additionally, Service Providers must ensure that threat signatures are regularly updated across all IT systems. [I] 2. The Service Provider shall implement appropriate SIEM tools or subscribe to SIEM services to collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.	Cybersecurity framework And Subscription to EPP, EDR, XDR etc. and SIEM platforms	TIER 3
GC-SCRM.S1; GC-SCRM.S2; GC-SCRM.S4; GC-SCRM.S5; GC-SCRM.S9;	GC-SCRM (Supply Chain Risk Management); CM-ED (External Dependencies/Supply Chain/Procurement);	[B] The Service providers shall manage cyber risks associated with suppliers and external dependencies: [B] 1. Service Providers shall develop a supply chain risk management strategy highlighting the supply chain risk assessment process for Suppliers and third-party service providers of information systems, hardware, and network components.	Cybersecurity framework and/or Third-party risk management strategy	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
GC-SCRM.S10; GC-SCRM.S11; GC-SCRM.S13; CM-ED.S1; CM-ED.S9; CM-ED.S11; CM-CH.S12	CM-CH (Cyber Hygiene)	[B] 2. The contract with Service Providers must include a clause which aligns the Service Provider's cybersecurity objectives with the risks embedded or inherent in the service to be provided.		
CRM-SAIS.S5; CRM-SAIS.S6; CRM-RA.S4; GC-SE.S6; GC-RRA.S8; CM-CH.S13	CRM-SAIS (Situation Awareness & Info Sharing); CRM-RA (Risk Assessment); GC-SE (Sector Environment); GC-RRA (Roles, Responsibilities & Authorities); CM-CH (Cyber Hygiene)	[B] 1. The Service providers shall perform cyber threat and vulnerability monitoring and remediation. [I] 2. The Service Provider shall implement appropriate monitoring tools or subscribe to MSSP services to collect, manage, and analyse events that could help detect, understand, or and remediate vulnerabilities. [I] 3. The Service Provider shall maintain active membership of the CS-ISAC [B] 4. Service Providers shall maintain active threat intelligence information sharing with relevant stakeholders like peer Service Providers, vendors, service providers, NCC-CSIRT, and National Authorities. [B] 5. Service Providers shall maintain active communication with dedicated sectoral CIRT/CSIRT/SOC or equivalent (e.g., NCC-CSIRT) for overseeing sector-specific IT security, monitoring and analyzing cyber threats, and issuing warnings and alerts regarding potential or ongoing attacks.	Subscription to MSSP platforms Subscription to NCC-CSIRT threat intel platforms	TIER 3
CCB-CECC.S1; CCB-CECC.S2; CCB-CECC.S3;	CCB-CECC (Cybersecurity Ecosystem & Cross-	[B] The Service providers shall participate in cybersecurity stakeholders' activities to inform, collaborate, share, and advance cybersecurity services within the communications sector by:	Compliance evidence	TIER 3

STANDARDS	PILLAR ELEMENTS	GUIDANCE NOTES	ARTIFACTS	TIER
<i>Tier 1: Core networks, spectrum holders, all communication service providers / Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers / Tier 3: Support service providers to other communication service providers</i>				
[B] = Baseline [I] = Intermediate [F] = Full				
CCB-CRD.S1; CCB-CRD.S2; CM-CH.S14	Sector Cooperation); CCB-CRD (Cybersecurity Research & Development); CM-CH (Cyber Hygiene)	[F] • The Service Provider shall participate in initiatives related to cybersecurity or collaborate with academic institutions, NGOs, innovation hubs, professional organizations, international development agencies, and others to strengthen the sector's cybersecurity ecosystem.		

TIER 1: Core networks, spectrum holders, all communication service providers | Tier 2: National coverage, shared infrastructure, aggregate & emerging tech providers | UASL (MNO)

**PILLAR 1: GOVERNANCE AND COMPLIANCE (GC)
(GUIDANCE NOTES)**

Governance and Compliance (GC)

GC-LR.S1	GC-LR: Laws and Regulations	[B] 1. Service Providers shall retain call logs, user IDs, and traffic data in-country for at least 2 years. Service Providers shall provide such data to relevant security agencies upon the presentation of a valid law enforcement warrant. [B] 2. Service Providers shall notify the NCC of significant system breaches within four (4) hours using the template provided in Annexure I [B] 3. Service Providers shall demonstrate the implementation of systems to prevent network use for cybercrime (e.g., fraud, hate speech) and cooperate with investigations [B] 4. Service Providers shall develop an implementation plan of secure infrastructure against unlawful interference.	Evidence of Compliance	Tier 1&2
GC-LR.S2; GC-LR.S3; GC-LR.S4	GC-LR: Laws and Regulations	[B] 1. Service Providers shall appoint a DPO registered with the Nigeria Data Protection Commission (NDPC). [B] 2. Service Providers shall report breaches of personal data to NDPC and NCC in line with the NDPA [B] 3. Service Providers shall store personal and SIM data and make it accessible to NCC upon request. [B] 4. Service Providers shall be required to conduct Data Protection	Evidence Of Compliance	Tier 1&2

		Impact Assessments (DPIAs) for high-risk processing (e.g., biometric collection, AI-driven analytics). [B] 5. Service Providers shall maintain detailed Records of Processing Activities (RoPA) and conduct annual audits.		
GC-LR.S5	GC-LR: Laws and Regulations	[B] 1. Service Providers shall implement adequate measures to protect communication infrastructure from cyber threats. [B] 2. Service Providers shall directly report cyber incidents targeting CNII to NCC-CSIRT.	Cybersecurity Framework/Policy, Evidence of Incident Reported	Tier 1&2
GC: SE - Sector Environment				
GC-SE.S1	GC-SE: Sector Environment	[B] 1. Service Providers should register and participate in Information Sharing Analysis Centre (ISAC) activities as defined from time to time. [B] 2. Service Providers shall subscribe or access cyber threats news, bulletins and alerts from relevant organizations and entities.	CS-ISAC membership, Evidence of Subscription/Receipts of such bulletins and alerts.	Tier 1&2
GC-SE.S2	GC-SE: Sector Environment	[B] Service Providers shall demonstrate an understanding of role(s) regarding critical systems and responsibilities and communicate such within their organization.	List of Critical IT Assets, Ownership and Maintenance.	Tier 1&2
GC-SE.S3; GC-SE.S4; GC-SE.S6	GC-SE: Sector Environment	[B] Service Providers shall establish and demonstrate an approved cybersecurity framework that emphasizes key resilience requirements for critical services across all operational conditions, including during times of crisis, attack and disasters, throughout the recovery process, and during normal operations.	Approved cybersecurity framework/strategy	Tier 1&2
GC-SE.S5	GC-SE: Sector Environment	[B] Service Providers shall ensure sufficient understanding of the risks of legacy, refurbished, end of support, non-type approved equipment and assets.	Inventory and risk treatment plan for legacy, refurbished and end of support equipment and assets.	Tier 1&2
GC-SE.S6	GC-SE: Sector Environment	[B] Service Providers shall maintain active threat intelligence information sharing with relevant stakeholders like peer Service Providers, vendors, NCC-CSIRT, and National Authorities (ONSA, NCCC, Nigeria Police, DSS, etc.)	CS-ISAC Membership, Evidence of Active Subscription	Tier 1&2

GC: RRA - Roles, Responsibilities and Authorities

GC-RRA.S1	GC-RRA: Roles, Responsibilities and Authorities	[B] Service Providers shall conduct cybersecurity awareness sessions/briefings at least twice a year for Board Members and senior management to foster a culture that is risk-aware, cybersecurity-conscious, and dedicated to continuous improvement.	Cybersecurity training report for board	Tier 1&2
GC-RRA.S2	GC-RRA: Roles, Responsibilities and Authorities	[B] Service Providers shall develop organisational measures to communicate and enforce cybersecurity issues by putting in place: • Clear role and accountability frameworks for cybersecurity matters in the organisation • Communication framework(s) on cybersecurity matters to educate and inform staff on cybersecurity matters on an ongoing basis • Develop an accountability framework that refers cybersecurity issues to designated authority(ies).	Cybersecurity risk management framework & implementation evidence.	Tier 1&2
GC-RRA.S3; GC-RRA.S4; GC-RRA.S5	GC-RRA: Roles, Responsibilities and Authorities	[B] 1. The Service Providers shall appoint a senior official or management personnel and alternate officer (hereafter referred to as the “Designated Officer”) responsible for assessing, identifying, and mitigating cybersecurity risks, responding to incidents, establishing appropriate standards and controls, and overseeing the development and execution of processes and procedures in accordance with the cybersecurity and cyber resilience policy or framework approved by the Board, Partners, or Proprietor. [B] 2. This designated officer shall bear the title of a Chief Information Security Officer (CISO) [B] 3. Service Providers shall establish a reporting procedure to ensure the timely communication of cybersecurity incidents or unusual activities within the organization to the Designated Officer, in accordance with the timeframes specified by guidelines, policies, laws, circulars, frameworks, or other relevant directives issued by the NCC. [B] 4. Service Providers designated as Critical National Information Infrastructure (CNII) owner or Service Providers in accordance with the Official Gazette on the Designation and Protection of CNII Order, 2024, shall define the roles and responsibilities of the Chief Information Security	NCC acknowledgement of CISO appointment, Job description of the nominated or appointed CISO	Tier 1&2

		Officer (CISO) in alignment with the guidelines outlined in the same Official Gazette. [B] 5. The CISO of the Service Providers shall report to leadership of the organisation. In addition, CISO shall possess sufficient qualification and skills to carry out his/ her responsibilities. [B] 6. The CISO shall have sufficient authority within the organisation.		
GC-RRA.S6	GC-RRA: Roles, Responsibilities and Authorities	[B] 1. Service Providers shall conduct reference checks prior to the appointment of major suppliers and ensure that these suppliers or third-party service providers sign a Non-Disclosure Agreement (NDA) and undergo a cybersecurity compliance audit for major third-party service providers. [B] 2. Service Providers shall establish and sign confidentiality and integrity agreements with third-party service providers and conduct due diligence on all such providers accessing their IT systems	Reference check, NDA with key third-party service providers.	Tier 1&2
GC-RRA.S7	GC-RRA: Roles, Responsibilities and Authorities	[B] Service Providers shall include cybersecurity training awareness in the induction programmes of new employees and on an ongoing basis	Evidence of cybersecurity awareness session	Tier 1&2
GC-RRA.S8	GC-RRA: Roles, Responsibilities and Authorities	[B] Service Providers shall maintain active communication with NCC-CSIRT for overseeing sector-specific IT security, monitoring and analysing cyber threats, and issuing warnings and alerts regarding potential or ongoing attacks.	Acknowledgement of communication with NCC-CSIRT	Tier 1&2
GC: PP - Policies and Procedures				
GC-PP.S1	GC-PP: Policies and Procedures	[B] 1. For the purpose of managing risks to systems, networks, and databases arising from cyberattacks and threats, Service Providers shall develop a comprehensive Cybersecurity and Cyber Resilience policy document aligned with the NCC Framework. Any deviations from the NCC Framework shall be documented, with explanations for such deviations (whether technical or otherwise) clearly outlined within the policy document. [B] 2. The policy document shall require approval from the Board, Partners, or Proprietor of the Service Providers. The aforementioned group	Cyber Resilience policy documents	Tier 1&2

		shall review the policy at least once a year to enhance and strengthen the organization's cyber resilience posture.		
GC-PP.S2	GC-PP: Policies and Procedures	[B] 1. Service Providers shall have policies (including but not limited to) 3rd party data/supply chain security management, Access Control, VAPT, Asset ownership and management; including architectural design, in life management, commissioning internet facing assets, and decommissioning, configuration management, Business continuity management, Cloud security, encryption policies and Cryptographic material management, Device, system, network asset and other endpoint security, Authentication policies, Authorization policies and processes, Information classification and handling, network segmentation/ isolation policies, Personnel security, PII and privacy policies,, Physical security, Risk management, Security incident management; including breach notification, analysis and mitigation planning, Change management, Security monitoring; including reporting to compliance programme, Secure software development life cycle management, Software security update management including patch management, Staff training and awareness, Vulnerability disclosure management, Cybersecurity control management policy etc. [B] 2. Service Providers shall develop a policy for mobile and web applications and related services, subject to approval by their Board, Partners, or Proprietor. This policy must cover parameters for any "new product," including its alignment with the overall business strategy, inherent risks, risk management and mitigation measures, regulatory compliance, and customer experience. Additionally, it shall explicitly incorporate security requirements from the perspectives of Functionality, Security, and Performance (FSP). [B] 3. These policies shall include related organization's use of information assets, such as desktops, laptops, BYOD devices, networks, internet, data, and similar resources. The aforementioned policies may either be integrated into the Service Providers' overarching cybersecurity policy or issued as standalone policies. [B] 4. Service Providers shall incorporate best practices from standards	Policy documents Up to date international standards	Tiers 1&2

		such as ISO 27001, ISO 27002, and their subsequent revisions, as applicable, and update their practices accordingly		
GC-PP.S3	GC-PP: Policies and Procedures	[B] The cyber resilience policy(ies) of Service Providers shall be reviewed at least yearly, and a version control process shall be established to support this review.	Updated cyber resilience policy	Tiers 1&2
GC-PP.S4	GC-PP: Policies and Procedures	[B] 1. The Cybersecurity Framework shall include the following process to identify, assess, manage, communicate and ensure compliance with cybersecurity risks associated with personnel, processes, information, networks, and systems: a. ‘Governance’ oversight responsibilities related to managing cybersecurity risks in the organisation. b. ‘Risk Management’ of critical IT and OT assets and risks associated with such assets. c. ‘Cybersecurity Profiling’ to deploy suitable controls, tools, and measures. d. ‘Detection, Response and Resilience’: i. Detecting incidents, anomalies, and attacks through appropriate monitoring tools/processes. ii. Response by taking immediate steps after identification of the incident, anomaly, or attack. iii. Recovery from incident through incident management and other appropriate recovery mechanisms. e. Cybersecurity Training: to empower users and key personnel in cybersecurity, cyber awareness and cyber hygiene.	Up to date Cyber resilience policy documents And/or Cybersecurity Framework	Tier 1&2
GC-PP.S5	GC-PP: Policies and Procedures	[B] Service Providers shall apply the Plan-Do-Check-Act (PDCA) cycle or other applicable management practices when creating and utilizing documented information. For example, activities in the ‘Plan’ phase shall be guided by policies; the ‘Do’ phase will follow procedures (SOPs); and the ‘Check’ and ‘Act’ phases will refer back to the policies and procedures to ensure continuous improvement.	Up to date Cyber resilience policy documents	Tier 1&2

GC-PP.S6	GC-PP: Policies and Procedures	[B] The chain of command for any approval process of asset ownership and custodianship in the organization concerning cybersecurity should be clearly defined and approved.	Approved asset register	Tier 1&2
GC-PP.S7	GC-PP: Policies and Procedures	[B] 1. The cybersecurity policy shall encompass the principles prescribed by National Cybersecurity Policy and Strategy and the Official gazette on designation and protection of CNNI order, 2024 [B] 2. As part of their compliance with the CRF NCS, Service Providers shall incorporate, the following key aspects including but not limited to: a. Assess Compliance with applicable guidelines/ policies/ laws/ circulars/ regulations, etc. issued by NCC. b. Develop compliance policies, procedures and SOPs c. Implement controls such as security measures d. Train employees on compliance management e. Monitor and review compliance management processes f. Regular compliance audits and reporting.	Evidence of Compliance	Tier 1&2
GC-PP.S8	GC-PP: Policies and Procedures	[B] The Board, Partners, or Proprietor of the Service Providers shall establish a Cybersecurity Committee consisting of experts proficient in cybersecurity. This committee shall meet bi-annually to review the implementation of the cybersecurity and cyber resilience policy approved by the Board, Partners, or Proprietor. The review process shall include setting goals for a target level of cyber resilience and developing a plan to enhance and strengthen cybersecurity and cyber resilience. The outcomes of these reviews shall be presented to the Board, Partners, or Proprietor of the Service Providers for appropriate action.	Board extracts of decisions on cybersecurity	Tiers 1&2
GC: OV – Oversight				
GC-OV.S1; GC-OV.S2	GC-O: Oversight	[B] 1. The Board/Oversight arm of the Service Providers shall constitute a Cybersecurity Committee comprising experts proficient in technology. This Committee shall meet bi-annually to review the implementation of the cybersecurity and cyber resilience policy approved by their Board/Partners/Proprietor. Such reviews shall define target levels of cyber	Board extracts of decisions on cybersecurity	Tiers 1&2

		resilience and detail strategic plans for strengthening cybersecurity postures. The findings shall be presented to the Board, Partners, or Proprietor of the Service Providers to facilitate appropriate action. [B] 2. The cybersecurity committee and the senior management of the Service Providers, including the CISO, shall at minimum quarterly review any cybersecurity incidents or attacks and proactively take measures to enhance cybersecurity and cyber resilience.		
GC-OV.S3	GC-O: Oversight	[B] 1. As part of compliance management with respect to this framework, Service Providers shall apply the following key aspects (including but not limited to) for implementing compliance management: a. Assess Compliance with applicable guidelines/policies/laws/circulars/regulations, etc., issued by NCC. b. Develop compliance policies and procedures c. Implement controls such as security measures d. Train employees e. Monitor and review compliance management processes f. Regular audits and reporting.	Cyber risk management framework	Tiers 1&2
GC-OV.S4	GC-O: Oversight	[F] 1. Service Providers shall regularly conduct cyber resilience reviews and evaluations using the Cybersecurity Capability Index (CCI) and submit relevant evidence to the NCC twice every six months. [F] 2. Service Providers shall use relevant metrics defined in the CRF NCS for measuring their cybersecurity maturity level.	CCI report	Tier 1&2
GC: SCRM - Supply Chain Risk Management				
GC-SCRM.S1; GC-SCRM.S2; GC-SCRM.S5; GC-SCRM.S9	GC-SCRM: Supply Chain Risk Management	[B] Service Providers shall develop a supply chain risk management strategy highlighting the risk assessment process for Suppliers and third-party service providers of information systems, hardware, and network components and communicate same to NCC	Supplier risk management strategy	Tier 1&2
GC-SCRM.S3; GC-SCRM.S4;	GC-SCRM: Supply Chain Risk Management	[B] When a core network, OSS/BSS, back-office systems, customer-facing applications, ICT infrastructure, and others, of a Service Provider are managed by a third-party the Service Providers shall instruct the third-party	Supplier risk management strategy and/or Third-party agreement	Tier 1&2

GC-SCRM.S6; GC-SCRM.S8		providers to comply with the applicable guidelines outlined in the CRF NCS. Additionally, the Service Providers shall obtain the necessary cyber audit certifications from these providers to verify their adherence and ensure overall compliance with the framework.		
GC-SCRM.S5	GC-SCRM: Supply Chain Risk Management	[B] The supply chain risk management plan must highlight sections containing essential measures which aligns with the cyber resilience objectives of the Service Providers and the risk profile/assessment of the contractor or third-party provider.	Supplier risk management strategy	Tier 1&2
GC-SCRM.S7	GC-SCRM: Supply Chain Risk Management	[I] 1. Service Providers shall acquire and obtain SBOMs for any new and existing critical systems, software products or Software-as-a-Service (SaaS) applications. These SBOMs should include details such as all open-source and third-party components present in the codebase, versions of the components used, their patch status, and other relevant information. This enables security teams to efficiently identify and address any security or licensing risks associated with the software. [I] 2. SBOM shall include (but not limited to) the following: a. License information b. Name of the supplier c. All primary (top level) components with all their transitive dependencies, including in-house or outsourced (open source or proprietary components) and relationships d. Encryption used e. Cryptographic hash of the components f. Frequency of updates g. Known unknown (where a SBOM does not include a full dependency graph) h. Access control i. Methods for accommodating occasional incidental errors.	SBOM	Tier 1&2
GC-SCRM.S9	GC-SCRM: Supply Chain Risk Management	[B] 1. Any single third-party service provider serving multiple Service Providers poses a concentration risk. If such providers experience cybersecurity incidents or attacks, it could have systemic implications due to the high concentration risk. Therefore, Service Providers should consider	Cybersecurity Framework	Tier 1&2

		and assess this concentration risk when outsourcing multiple critical services to the same third-party provider. [B] 2. Service Providers shall identify third-party service providers that pose a concentration risk and implement specific cybersecurity controls, including independent audits of their systems and protocols, to mitigate this risk. Additionally, Service Providers shall verify that these third-party providers are meeting the operational resilience objectives outlined in the CRF NCS.		
GC-SCRM.S10; GC-SCRM.S13	GC-SCRM: Supply Chain Risk Management	[B] Service Providers shall comply with internationally recognised standards and frameworks on supply chain risk management such as NISTIR 8276	Framework/standard certification	Tier 1&2
GC: BS - Budget and Spending				
GC-BS.S1; GC-BS.S2; GC-BS.S3; GC-BS.S4	GC-BS: Budget and Spending	[F] 1. Service Providers shall allocate an adequate percentage of the total company budget to cybersecurity. This allocation shall be designated under a separate budgetary category to facilitate monitoring and oversight by the Board of Directors and top-level management. [F] 2. Service Providers shall ensure that adequate and sufficient resources are allocated and aligned with the cybersecurity risk strategy, roles, responsibilities, and policies. These resources should be specified in terms of budget, personnel, and materials. Resourcing needs shall be reviewed regularly, based on the progress or gaps in implementing cybersecurity standards, and any updates shall be reflected in the budgetary allocations. [F] 3. The Service Providers has an operational procedure to track cybersecurity budget expenditures and adjusts future budgets accordingly to meet the resiliency goal of the organisation.	Approved document showing budgetary provisions for cybersecurity	Tier 1&2
GC-BS.S1; GC-BS.S2; GC-BS.S3; GC-BS.S4	GC-BS: Budget and Spending	[F] 1. Service Providers shall allocate an adequate percentage of the total company budget to cybersecurity. This allocation shall be designated under a separate budgetary category to facilitate monitoring and oversight by the Board of Directors and top-level management. [F] 2. Service Providers shall ensure that adequate and sufficient	Approved document showing budgetary provisions for cybersecurity	Tier 1&2

		resources are allocated and aligned with the cybersecurity risk strategy, roles, responsibilities, and policies. These resources should be specified in terms of budget, personnel, and materials. Resourcing needs shall be reviewed regularly, based on the progress or gaps in implementing cybersecurity standards, and any updates shall be reflected in the budgetary allocations. [F] 3. The Service Providers has an operational procedure to track cybersecurity budget expenditures and adjusts future budgets accordingly to meet the resiliency goal of the organisation.		
GC: RM - Risk Management Strategy				
GC-RM.S1; GC-RM.S2; GC-RM.S4; GC-RM.S5	GC-RM: Risk Management Strategy	[B] 1. The design of the cyber risk management framework should encompass, but not limited to, the following aspects: • Identification of cybersecurity risks facing the organization • Classification of identified and mapped business functions, supporting processes, and information assets at risk • Establishment of the organization's risk appetite for IT and cybersecurity threats • Definition of mitigation measures and controls to reduce identified risks • Continuous monitoring of the effectiveness of these measures and controls • Assessment of the impact of major changes and significant operational, technical, or cybersecurity incidents on the risk landscape. [B] 1. Service Providers should consider utilizing the latest versions of Information Security Management Standards (ISMS) as guidance for the design, implementation, and ongoing maintenance of their information security risk management processes. [B] 2. The risk management strategy of Service Providers shall encompass, but not limited to, risk assessment, risk analysis, risk mitigation, ongoing risk monitoring and review. In addition, other activities include compliance with applicable laws and regulations, communication of risk management policies to all stakeholders, implementation of effective mitigation measures with alternative controls where feasible, efforts to	Cyber risk management framework, ISO certification Outcome of monitoring	Tiers 1&2

		reduce residual risk, and ensuring that cybersecurity risk tolerance remains within acceptable limits.		
GC-RM.S3	GC-RM: Risk Management Strategy	[F] Comprehensive, scenario-based testing shall be conducted to evaluate the cybersecurity risks faced by the Service Providers. Each Service Provider shall develop attack scenarios aligned with their business model and assess their risks accordingly taking into consideration the critical services provided by the Service Providers as designated in the official gazette on Critical National Infrastructure. Refer to Annexure XII for a sample list of potential attack scenarios and corresponding possibilities.	Cyber risk management framework	Tiers 1&2
GC: CP – Compliance				
GC-CP.S1; GC-CP.S2; GC-CP.S3	GC-C: Compliance	[B] The Service Providers shall comply with all relevant provisions of the CRF NCS and shall demonstrate evidence of on-going compliance as issued by NCC.	Cybersecurity Audit/ Assessment Report	Tier 1&2
GC-CP.S4	GC-C: Compliance	[B] Service Providers are encouraged to comply with relevant international cybersecurity standards and frameworks.	Relevant international cybersecurity certifications	Tier 1&2
PILLAR 2: CYBER RISK MANAGEMENT (GUIDANCE NOTES)				
CRM: AR - Asset and Risk Management				
CRM-AR.S1; CRM-AR.S2; CRM-AR.S4; CRM-AR.S6	CRM-AR: Asset and Risk Management	[B] 1. All Service Providers shall identify and classify their critical systems in accordance with this framework, based on their criticality as a designated national asset as classified under the Presidential Order on CNII, sensitivity and importance to business operations. The Board, or oversight arm of the Service Providers must approve the list of critical systems. [B] 2. All Service Providers shall keep an up-to-date inventory of their hardware and systems, software, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets),	Approved asset list Outcome of criticality assessment	Tier 1&2

		interfacing systems (both internal and external), network resources, network connections, encryption methods, and data flows. [B] 3. Any additions, deletions, or modifications to existing assets shall be updated in the asset inventory within three working days. [B] 4. To conduct the criticality assessment of assets, Service Providers shall undertake the following steps (including but not limited to): - Maintain a comprehensive asset inventory - Conduct a vulnerability assessment [B] 1. Service Providers shall develop and maintain an up-to-date network architecture diagram at the organizational level, encompassing both wired and wireless networks. [F] 2. Service Provider shall conduct threat modelling based on risk assessment.		
CRM-AR.S2	CRM-AR: Asset and Risk Management	[B] Service Providers shall be required to keep an inventory of organisational communication, data flows, and encryption methods across all IT systems and network resources.	IT asset inventory	Tiers 1&2
CRM-AR.S3	CRM-AR: Asset and Risk Management	[B] Service Providers shall perform regular audits and inspections of their IT and OT resources to ensure that there are not any rogue or shadow assets in the service providers environment.	IT Audit report, IT asset inventory	Tier 1&2
CRM-AR.S5	CRM-AR: Asset and Risk Management	[B] Service Providers shall put in place a database approach to: - Understand and inventorise their IT logical and physical assets - Understand which data or systems are most critical for providing critical services as well as any associated interdependencies.	Data asset inventory	Tier 1&2
CRM-AR.S7; CRM-AR.S8	CRM-AR: Asset and Risk Management	Risk Management Framework [B] 1. The design of the cyber risk management framework needs to consider the following (including but not limited to): • Identification of the cybersecurity risk for the organisation • Classification of identified and mapped business functions, supporting processes and information assets at risk. • Determination of risk appetite for IT and cybersecurity risks. • Definition of mitigation measures and controls to reduce the risks.	Cyber risk management framework/strategy, Cybersecurity Maturity Matrix Outcome of monitoring	Tier 1&2

		• Monitoring of the effectiveness of the above-mentioned measures and controls. • Evaluation of the effect of major changes and significant operational, technical or cybersecurity incident(s) on the risks. [B] 2. Service Providers should consider using the latest version of Information Security Management Systems (ISMS) as a guideline for the design, implementation, and ongoing maintenance of information security risk management processes. [B] 3. The risk management strategy of Service Providers shall encompass, but not limited to, risk assessment, risk analysis, risk mitigation, ongoing risk monitoring and review. In addition other activities include compliance with applicable laws and regulations, communication of risk management policies to all stakeholders, implementation of effective mitigation measures with alternative controls where feasible, efforts to reduce residual risk, and ensuring that cybersecurity risk tolerance remains within acceptable limits. [F] 4. Service Providers shall utilize metrics such as (including but not limited to) MTTD (Mean Time to Detect), MTTR (Mean Time to Respond), MTTC (Mean Time to Contain), the number of cybersecurity incidents or intrusion attempts detected and resolved within a specified period, the number of false positives and false negatives generated by cybersecurity monitoring tools, the number of successful cyber-attacks in the past year, and the progress made in reducing these figures through ongoing refinement of monitoring processes to assess their cybersecurity maturity level. [B] 5. Service Providers shall periodically evaluate the level of employee cybersecurity awareness, for example, by measuring metrics such as phishing test success rates, Business Email Compromise (BEC) success rate, among other indicators [B] 6. Service Providers shall conduct regular IT asset management activities, including tracking the number of devices on the network operating outdated or end-of-life (EOL) software, devices no longer receiving security updates, unidentified devices connected to the internal network, and the integration of third-party devices and services. Additionally, IT asset		
--	--	---	--	--

		management should encompass processes related to managing asset access and permissions, patching schedules, security ratings, third-party security ratings, and the number of known vulnerabilities.		
CRM-AR.S8	CRM-AR: Asset and Risk Management	[B] All Service Providers shall develop their risk management framework in alignment the common methodology defined at the sectoral and/or national level.	Cyber risk management framework/strategy	Tier 1&2
CRM: SAIS - Situation Awareness and Information Sharing				
CRM-SAIS.S1; CRM-SAIS.S2; CRM-SAIS.S3; CRM-SAIS.S4	CRM-SAIS: Situation Awareness and Information Sharing	[B] Vulnerability Assessment and Penetration Testing (VAPT) shall be conducted to identify vulnerabilities within the IT & OT environments, including all critical systems, infrastructure components, and other IOT systems as outlined in this framework. A comprehensive VAPT scope has been specified to guide this activity (see Annexe III). For every production release, a vulnerability assessment shall be performed. Additionally, for all major releases, the Service Providers shall conduct VAPT to evaluate the risks and vulnerabilities resulting from recent updates or modifications to applications and software.	Up-to-date VAPT report, Change Management Policy	Tier 1&2
CRM-SAIS.S5	CRM-SAIS: Situation Awareness and Information Sharing	[I] The Service Providers shall maintain active membership of the CS-ISAC and other 3rd party Threat Intelligence Platforms.	CS-ISAC active Membership, Other 3rd party Threat Intelligence Platforms.	Tier 1&2
CRM-SAIS.S6	CRM-SAIS: Situation Awareness and Information Sharing	[B] Service Providers shall be onboarded to NCC-CSIRT to enhance situational awareness of current and emerging cybersecurity threats and to facilitate timely information sharing, enabling individual entities to take proactive, preventive, and protective measures.	Auditable evidence of reporting	Tier 1&2
CRM-SAIS.S7	CRM-SAIS: Situation Awareness and Information Sharing	[B] All cybersecurity incidents shall be reported in a timely manner through the incident reporting portal according to the provisions of the CRF NCS.	Incident Reports	Tier 1&2

CRM: RA - Risk Assessment				
CRM-RA.S1; CRM-RA.S7	CRM-RA: Risk Assessment	[B] Service Providers shall identify potential cyber risks they may encounter, assess the likelihood of associated threats and their impact on their business, and implement risk responses and controls proportional to the criticality of these risks.	Cyber risk assessment report	Tier 1&2
CRM-RA.S2; CRM-RA.S3	CRM-RA: Risk Assessment	[I] 1. Service Providers shall perform a risk assessment of their organization's IT environment, including post-quantum risks, every six months for Tier 1 Service Providers and annually for qualified and mid-size Service Providers (Tiers 2 & 1). This assessment aims to provide visibility and a reasonably accurate evaluation of the overall cybersecurity risk posture. The Service Providers shall use the results of this risk assessment to develop a measurable cybersecurity risk score. [I] 2. Risk Assessment shall include (but not limited to): a. Technology stack and solutions used b. Known vulnerabilities c. Dependence on third-party service providers d. Data storage, security, and privacy protection e. Threats, likelihoods, and associated risks	Cyber risk assessment report	Tier 1&2
CRM-RA.S4	CRM-RA: Risk Assessment	[B] 1. Service Providers shall implement Dark Web monitoring (for brand intelligence, customer protection, etc.) and may utilize legitimate takedown services as part of their cyber-defense strategy to detect and address brand abuse, data or credential leaks, and to combat cyber threats. [B] 2. Service Providers shall devise Standard Operating Procedures (SOPs) to analyse and implement the advisories issued by ngCERT, NCC-CSIRT, or any other government agency within a defined timeframe as specified in the SOP. [B] 3. Service Providers shall have processes in place to manage and incorporate IOAs/IOCs/malware alerts/vulnerability alerts received from	SOPs for implementing threat advisories and alerts Evidence of CSIRT on boarding Evidence of monitoring cyber space Updated Subscription	Tier 1&2

		NCC-CSIRT (as applicable) or any other government agencies [B] 4. Service Providers shall be onboarded to NCC-CSIRT intelligence platform to share and receive threat advisories for necessary action and implementation. [B] 5. Service Providers shall subscribe to anti-phishing/ anti-rogu app services of DNSSEC to mitigate potential phishing or impersonation attacks. [B] 6. Service Providers shall proactively monitor the cyberspace to identify phishing websites by subscribing to DNSSEC services to monitor their domains and report the compromises to NCC-CSIRT for taking appropriate action.		
CRM-RA.S5; CRM-RA.S6	CRM-RA: Risk Assessment	[B] A risk assessment shall be conducted to gain insight into the Service Providers' threats, vulnerabilities, and their potential impacts. This includes an assessment of authentication-based solutions to gain insights into the context behind each login. Additionally, when a user attempts to sign in, a risk-based authentication system shall analyze factors such as device, location, network, and sensitivity to assess the associated risks.	Cyber risk assessment report	Tier 1&2
CRM-RA.S8	CRM-RA: Risk Assessment	[F] Service Providers shall maintain valid cybersecurity insurance (where applicable) for critical assets to ensure comprehensive risk mitigation and financial loss protection.	Valid cybersecurity insurance	Tier 1&2

PILLAR 3: CYBERSECURITY MEASURES (GUIDANCE NOTES)

CM: DP - Data Privacy

CM-DP.S1; CM-DP.S2; CM-DP.S3	CM-DP: Data Privacy	[B] 1. Service Providers shall deploy encryption/data masking tools, access controls to physical and logical assets, and conduct regular security assessments to safeguard both physical and logical assets against unauthorized access and potential breaches. [B] 2. Service Providers shall establish clear data handling policies,	Access Control Policy, Data Protection Compliance Certificate	Tier 1&2
------------------------------------	---------------------	--	---	----------

		employee training, and incident response plans in line with the provisions of the NDPA.		
CM-DP.S4	CM-DP: Data Privacy	[B] 1. Service Providers shall ensure that data is processed fairly, lawfully, and transparently, with legitimate purpose, proportionality, and data quality. [B] 2. Data Minimization: Service Providers shall collect and process only the minimum amount of data necessary for their services [B] 3. Transparency and Consent: Service Providers shall be transparent about data collection practices and obtain explicit consent from customers. [B] 4. Data Subject Rights • Access: Individuals have the right to access their personal data held by Service Providers. • Rectification: Individuals have the right to correct inaccurate or incomplete data. • Deletion: Individuals can request the deletion of their data under certain circumstances. • Objection: Individuals can object to the processing of their data. [B] 5. Service Providers shall appoint a DPO registered with the Nigeria Data Protection Commission (NDPC) in compliance with NDPA Act, 2023 [B] 6. Service Providers shall notify the NDPC and affected individuals within a specified timeframe following a personal data breach. [B] 7. Service Providers shall investigate the breach, identify the cause, and take steps to prevent future occurrences. [B] 8. Restrictions: Service Providers shall ensure that transfers of personal data outside Nigeria are in line with provisions of the NDPA Act 2023. [B] 9. Service Providers shall ensure that Data Protection Impact Assessments (DPIA) is conducted for high-risk processing (e.g., biometric collection, AI-driven analytics etc.)	Data Protection Compliance Certificate, Data Impact Assessment Report (s)	Tier 1&2
CM-DP.S5	CM-DP: Data Privacy	[B] Service Providers shall ensure compliance with privacy laws by embedding privacy principles into the core of any project involving personal data: 1. Service Providers shall implement technical, organizational, and	Data Protection Compliance Certificate	Tier 1&2

		governance measures to comply with all relevant local and national data privacy legislations. 2. Service Providers shall maintain detailed Records of Processing Activities (RoPA) and conduct regular audits to assess compliance with all relevant data privacy policies and procedures 3. Service Providers shall implement systems to continuously monitor data processing activities and identify potential risks.		
CM-DS.S1	CM-DS: Data Security	Data and Storage Devices security [F] 1. Data shall be protected through strong encryption methods during transmission (in motion), storage (at rest), and processing (in-use). For data in use, encryption shall be applied in cloud deployments (refer to Annexure-VIII). Wherever feasible, a layered approach combining Full-Disk Encryption (FDE) with File-Based Encryption (FBE) shall be adopted. Service Providers shall use industry-standard, robust encryption algorithms such as RSA and AES whenever encryption is implemented. Illustrative measures related to this are provided in Annexure-VI and Annexure-VII. [F] 2. To prevent data loss, Service Providers should deploy Data Loss Prevention (DLP) solutions or establish relevant processes. [B] 3. Service Providers shall implement measures to prevent unauthorized access to confidential data during the exchange and transfer of data with external parties. Illustrative measures to ensure security during data transmission over the internet are provided in Annexure-VII. [B] 4. Service Providers' information security policies shall also address the use of devices such as mobile phones, photocopiers, scanners, and other equipment that can be used to capture and transmit sensitive data within their IT infrastructure. This includes establishing access policies for personnel and defining network connectivity controls for these devices. [B] 5. To maintain data security, Service Providers shall validate and authorize all data storage devices before they are used within the IT infrastructure. Application Security in Customer Facing Applications: [B] Application security for customer-facing applications accessible over the	Encryption certificate or evidence of encryption. ISO/TS 27034 DLP licenses Data Protection Policy, Cybersecurity Framework/Strategy	Tier 1&2

		internet, portals containing sensitive or private information, and back-office applications that store financial and personal data provided by Service Providers to customers is of utmost importance. These applications present a significant attack surface due to their public availability for widespread use. Service Providers shall safeguard these internet-facing applications from cyber-attacks through appropriate cybersecurity measures as stipulated in the cybersecurity risk management framework/strategy. An illustrative list of measures to ensure security for such applications is provided in Annexure-V.		
CM-DS.S2	CM-DS: Data Security	[B] 1. Service Providers shall ensure that data related to compliance with the CRF-NCS is maintained in an accessible, readable, and usable form within the legal boundaries of Nigeria. [B] 2. During data classification, Service Providers shall comply with relevant data security standards, guidelines, and other government-issued policies, laws, circulars, and regulations, including those issued by NCC, NDPA, such as the NC Act 2003, the NDPA Act 2023, and any other applicable laws or regulations issued subsequently.	Evidence of compliance	Tier 1&2
CM-DS.S3	CM-DS: Data Security	[I] 1. Service Providers shall implement appropriate mechanisms, including the generation of relevant alerts, to monitor capacity utilization in real-time and proactively address any issues related to their capacity requirements. [B] 2. For capacity planning and monitoring, Service Providers shall adhere to the circulars and guidelines on capacity planning issued by NCC, including any updates from time to time.	Capacity utilisation report of critical services	Tier 1&2
CM-DS.S4	CM-DS: Data Security	[B] 1. It's essential that Service Providers shall ensure strong data protection, backup, and recovery measures are in place and actively enforced. [B] 2. Service Providers shall, by default, restrict administrative rights on end-user workstations, PCs, and laptops. Access rights shall only be granted on a need basis, subject to the established approval process, and limited to the specific duration required. [B] 3. Service Providers shall implement security controls for mobile and	Data Management Policy	Tier 1&2

		web applications that specifically address the handling, storage, and protection of Personally Identifiable Information (PII) and other business-related data. [B] 4. Service Providers' web and mobile applications shall not store sensitive information in HTML hidden fields, cookies, or any form of client-side storage, in order to prevent potential compromise of data integrity. [B] 5. Service Providers shall renew their digital certificates used in IT systems well in time. [B] 6. Service Providers shall implement appropriate controls to manage the use of VBA/macros in office documents and to restrict permissible attachment types within email systems. [B] 7. Service Providers shall maintain a documented data migration policy that outlines standard operating procedures (SOPs) and processes to be followed during data migration, ensuring data integrity, completeness, and consistency throughout the process.		
CM-DS.S5	CM-DS: Data Security	[B] 1. For the development of all software, applications, and feature enhancements, Service Providers shall ensure the establishment of separate production and non-production (test) environments. [B] 2. Following development and/or feature enhancements, Software Integration Tests (SIT) shall be conducted to verify that the entire software or application functions as intended. [F] 3. During the development phase of any software or application intended for use by Service Providers or their customers, it must be ensured that vulnerabilities identified by established best practices, such as OWASP guidelines or the top 25 software security vulnerabilities from SANS, are addressed. It is recommended that Service Providers adopt secure development methodologies, such as DevSecOps, to enhance the security of their applications and software.	ISO 27002 certification and/or cybersecurity framework	Tier 1&2
CM-DS.S6	CM-DS: Data Security	[F] 1. Service Providers shall acquire the source code for all critical applications from their third-party service providers. If obtaining the source code is not feasible, Service Providers shall establish a source code escrow agreement or an equivalent arrangement to effectively mitigate the risk of	ISO 27002 certification and or Escrow agreement	Tier 1&2

		provider default, continued access to the software's codebase and intellectual property. Additionally, Service Providers must ensure that all product updates, patches, and fixes are incorporated into the source code escrow agreement. [B] 2. For all software and applications where vulnerabilities may be identified at a later time, Service Providers shall ensure that these vulnerabilities are mitigated within a specified timeframe. Additionally, Service Providers shall include clear timelines in their Service Level Agreements (SLAs) with third-party service providers to ensure prompt compliance and resolution of identified vulnerabilities. [I] 3. Service Providers shall establish and implement risk assessment processes and controls for third-party service providers (including software vendors) that are appropriate to their criticality and associated risks, in order to effectively manage supply chain vulnerabilities. [B] 4. Service Providers shall ensure that maintenance and essential support for hardware and software applications, is formalized through an agreement.		
CM: IDAM - Identity & Access Management				
CM-IDAM.S1; CM-IDAM.S2; CM-IDAM.S3; CM-IDAM.S4; CM-IDAM.S7; CM-IDAM.S9	CM-IDAM: Identity & Access Management	[B] Access Controls, Password Policy/ Authentication Mechanism 1. No individual, regardless of rank or position, shall have an inherent right to access confidential data, applications, system resources, or facilities. Access shall be granted strictly based on defined roles, responsibilities, and approved authorization protocols. 2. Access to Service Providers' systems, applications, networks, databases, and other resources shall be granted only for a specified purpose and a defined period. Access to IT systems, applications, databases, and networks shall be on a need-to-know basis, adhering to the principle of least privilege. Such access shall be provided for a limited duration and secured through robust authentication mechanisms 3. User access rights, delegated access, unused tokens, and the activities of privileged users shall be reviewed regularly on a periodic basis.	Information security policy ISO 27001 Network Security Policy ISO 27001 Network Security Policy ISO 27001	Tier 1&2

		4. Access to external cloud services such as Dropbox, Google Drive, iCloud, OneDrive, and similar platforms shall be governed by the Service Providers defined policy and granted only in accordance with approved guidelines 5. Service Providers shall ensure that user access to critical systems is uniquely identifiable and properly logged whenever feasible, to facilitate auditing and review. These logs shall be securely stored for a minimum of two (2) years, with at least six (6) months retained in online mode and the remaining period in archival mode. Additionally, Service Providers must keep records of users accessing shared accounts. 6. Service Providers shall implement account access lock policies after failure attempts 7. Service Providers shall ensure that regular reviews of existing user accounts and access rights are conducted to identify dormant accounts, accounts with excessive privileges, unknown accounts, or any discrepancies. 8. Service Providers shall ensure that appropriate 'end of life' procedures are implemented for user management, including deactivating access privileges for users leaving the organization or whose access has been revoked. This applies to named user IDs, default user IDs, and generic email IDs. 9. Service Providers shall ensure that all critical systems accessible via the internet are protected with multi-factor security measures, such as VPNs, firewall controls, and multi-factor authentication (MFA). 10. Service Providers shall ensure that multi-factor authentication (MFA) is enabled for all users and systems accessing via online or internet connectivity, with particular emphasis on VPNs, webmail, and accounts that access critical systems from non-trusted environments to trusted environments. [B] Network Security Management 1. Service Providers shall ensure that appropriate controls are implemented to defend against viruses, malware, and ransomware attacks on servers and other IT systems. These measures may include host, network, and application-based intrusion prevention systems (IPS), customized		
--	--	---	--	--

		kernels for Linux, anti-virus and anti-malware software, and similar protections. Additionally, anti-virus definition files updates and automatic scans shall be performed regularly to maintain system security 2. Service Providers shall establish baseline standards to ensure consistent application of security configurations across OS, databases, network devices, enterprise mobile devices, and other components within the IT environment. Regular enforcement checks shall also be conducted to verify that these baseline standards are applied uniformly 3. Service Providers shall ensure that Local Area Networks (LAN) and wireless networks within the Service Providers' premises shall be secured through the implementation of appropriate access control measures. 4. Service Providers shall limit total and maximum connections to SMTP servers [B] Access Controls, Password Policy/ Authentication Mechanism 1. A Privileged Identity Management (PIM) solution or equivalent process shall be implemented to monitor, manage, and audit privileged access across systems and applications. 2. Service Providers shall establish and enforce an access control policy that includes strong password requirements for user access to systems, applications, networks, databases, and other IT resources. Illustrative examples and guidelines are provided in Annexure-G 3. Service Providers shall develop an Internet access policy to oversee and control the use of internet services, including social media platforms, cloud-based storage, and other related services within the critical IT infrastructure. 4. Service Providers shall implement controls and security measures to monitor staff with elevated system access privileges, such as administrative or privileged users. These measures shall include, but are not limited to, restricting the number of privileged users, conducting periodic reviews of their activities, preventing privileged users from accessing system logs that record their actions, and establishing strong controls over remote access by privileged users.		
--	--	--	--	--

CM-IDAM.S4	CM-IDAM: Identity & Access Management	No person by virtue of rank or position shall have any right to access confidential data applications, system resources or facilities. [B] Any access to Service Providers' systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. Access granted to IT systems, applications, databases and networks shall be on a need-to-use basis and based on the principle of least privilege. Such access shall be given for a specific duration and using effective authentication mechanisms	Cybersecurity Framework Zero Trust Implementation Plan	Tier 1&2
CM-IDAM.S5	CM-IDAM: Identity & Access Management	[B] Existing user accounts and access rights shall be periodically reviewed by the owner of the system in order to detect dormant accounts, accounts with excessive privileges, unknown accounts or any type of discrepancy.	Access Management policy ISO 37301:2021 (Compliance Management Systems)	Tier 1&2
CM-IDAM.S6	CM-IDAM: Identity & Access Management	[B] The Service Providers shall develop a comprehensive authentication policy for demonstrating that identities are proven, securely bound to credentials, and asserted during all interactions.	Authentication policy ISO 27001	Tier 1&2
CM-IDAM.S8	CM-IDAM: Identity & Access Management	[B] The Service Providers shall maintain a comprehensive log management policy	Log management policy ISO 27001	Tier 1&2
CM-IDAM.S10	CM-IDAM: Identity & Access Management	[B] 1. Physical access to the critical systems shall be restricted and provided only to authorized officials. Authorized employees shall properly supervise and accompany physical access provided to third-party service providers at all times. [B] 2. Employees of Service Providers shall be screened before granting access to organizational information and information systems. Physical access to the critical systems shall be revoked immediately if the same is no longer required. [B] 3. All Service Providers shall ensure that the perimeter of the critical equipment room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. wherever appropriate. [B] 4. Environmental controls (temperature, water, smoke, etc.), service	Physical Access Management Policy ISO 27001	Tier 1&2

		availability alerts (power supply, servers, etc.), access logs, etc. shall be monitored.		
CM-IDAM.S11; CM-IDAM.S12	CM-IDAM: Identity & Access Management	[B] 1. Original Equipment Manufacturers (OEMs), their service partners, and System Integrators offering remote support services to organizations, Service Providers must ensure that these services are properly governed and controlled. This includes maintaining logs and oversight of all activities carried out by remote support providers to ensure accountability and security. This control measure shall be complemented by regular monitoring and audits to ensure that the policies governing privileged users and remote access are consistently followed and strictly upheld. [B] 2. Service Providers must ensure the secure use of Remote Desktop Protocol (RDP) in IT systems. It should be implemented strictly on a need-to-use basis and must incorporate Multi-Factor Authentication (MFA). When remote access is necessary, it shall only be granted to authorized personnel from whitelisted IP addresses for a specified duration, with all activities being properly logged. [B] 3. Employees and third-party service providers granted authorized access to the Service Providers' critical systems, networks, and IT resources shall be subject to rigorous oversight, continuous monitoring, and strict access restrictions.	Information security policy ISO 27001/ ISO 27002	Tier 1&2
CM-IDAM.S13; CM-IDAM.S14	CM-IDAM: Identity & Access Management	[B] 1. Service Providers shall establish appropriate policies for the disposal of storage media and systems. [B] 2. Critical data and information on such devices shall be securely removed using methods such as wiping, cleaning, overwriting, degaussing, cryptographic shredding, or physical destruction, as applicable.	Information security policy ISO 27001	Tier 1&2
CM-IDAM.S15	CM-IDAM: Identity & Access Management	Endpoint Security [B] Service Providers shall implement solutions such as IPS to continuously monitor the organization's network for malicious activities. Usage of Active Directory (AD) or Equivalent servers [B] 1. Service Providers shall regularly review the AD or equivalent to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target of	Information security policy ISO 27001 VAPT Report	Tier 1&2

		attacks. [B] 2. Service Providers shall conduct penetration testing targeting known Domain Controllers' abuse attacks, with all identified vulnerabilities being promptly addressed and remediated as a top priority. Restricted use of removable media and electronic devices [B] Service Providers shall establish and enforce policies for the restricted and secure use of removable media (such as USB drives and external hard disks) and electronic devices (such as laptops and mobile devices). They shall also ensure that data is securely erased from these media and devices after use, so that no recoverable data remains. Secure Domain Controllers (DCs) Threat actors frequently target and leverage Domain Controllers (DCs) as staging points to facilitate the widespread distribution of ransomware across the network [B] 1. Service Providers shall ensure that Domain Controllers (DCs) are promptly patched whenever updates are released, and this process shall be reviewed quarterly to confirm that all patches have been successfully implemented [B] 2. Service Providers shall ensure that only necessary software is installed on Domain Controllers (DCs), as the presence of unnecessary applications can be exploited to execute arbitrary code on the system. [B] 3. Service Providers shall restrict access to Domain Controllers (DCs) to members of the Administrators group. Users within this group shall be kept to a minimum, and individuals shall use separate accounts with non-administrative permissions for daily operations [B] 4. Service Providers shall ensure that the firewalls on Domain Controller (DC) hosts are configured to block direct internet access.		
CM-IDAM.S16; CM-IDAM.S17	CM-IDAM: Identity & Access Management	[B] API Security API security safeguards against vulnerabilities and misconfigurations, preventing misuse of APIs. 1. Implementing effective security measures such as rate limiting and throttling during API development is essential to prevent overuse or abuse.	Information security policy ISO 27001 ISO/TS 23029 ISO 27001 ISO/TS 27034	Tier 1&2

		If Service Providers, the responsibility for ensuring API security lies with the service provider that provides and uses APIs. Service providers shall deploy appropriate API security solutions to protect the services and data transmitted through their APIs. 2. Proper access management, along with robust authentication and authorization measures, shall be implemented to ensure that only authorized entities can access the APIs 3. Service Providers shall follow the OWASP guidelines for API development, and the top 10 API security risks identified by OWASP shall be strictly addressed and mitigated. 4. Connecting to entities via APIs shall be strictly on a whitelist-based approach. [B] Mobile Application Security 1. The mobile application shall include root detection and root cloaking detection. Additionally, the application shall not operate on emulators or virtual devices. 2. Service Providers shall investigate the feasibility of implementing a mechanism that checks whether the device is rooted or jailbroken before installing the mobile application. The application should be disallowed from installation or operation on rooted or jailbroken devices, as well as on emulators or virtual devices. 3. Device policy enforcement features, including the detection of developer options, USB debugging, mock location, and manipulation of time settings, shall be implemented and configured accordingly. 4. The mobile application shall monitor and detect new network connections, including those to unsecured networks such as VPNs, proxies, and open Wi-Fi networks. 5. The mobile application shall incorporate anti-malware features to protect against threats such as application spoofing, Remote Access Trojans (RAT), screen mirroring attacks, overlay malware, keyloggers, tap jacking, and similar security risks. 6. Controls to prevent reverse engineering and application tampering shall be integrated into the mobile applications. These controls shall also include	
--	--	---	--

		runtime signature validation to ensure the authenticity of the application. 7. The mobile application shall perform checksum validation, and the checksum values of the application shall be made available in the public domain. 8. The mobile application shall detect the presence of active remote access, screen mirroring, ongoing voice calls, and other similar activities, and shall alert users accordingly to prevent online fraud. 9. The mobile application shall require re-authentication after a specified period of device inactivity and each time the user launches the application. 10. The mobile application shall not store or retain sensitive personal or customer authentication information, such as user IDs, passwords, keys, hashes, or hard-coded references, on the device. Additionally, the application shall securely erase any sensitive customer or user information from memory when the customer or user exits the application. 11. The mobile application shall be protected against common vulnerabilities, including SQL injection and other similar security threats. 12. Service Providers shall ensure that the use of raw SQL queries in the mobile application for fetching or updating data from databases is avoided. Additionally, sensitive information shall be stored in the database in an encrypted format. 13. The mobile application shall implement a device-binding solution to establish a unique digital identity, based on the device, mobile number, and SIM 14. OWASP MASVS shall be referred to for implementing mobile application security and other protective measures. 15. Service Providers shall consider implementing measures such as deploying a "containerized" app on mobile/smartphones for exclusive business use, which is encrypted and isolated from other smartphone data and applications. Additionally, measures to enable remote wiping of the containerized app, rendering its data unreadable in case of necessity, may also be considered. 16. Service Providers shall develop SOPs for the security of open-source		
--	--	---	--	--

		applications and address security concerns related to emerging technologies such as Generative AI.		
CM: NSG - Network Security (General)				
CM-NSG.S1	CM-NSG: Network Security (General)	[B] Service Providers shall ensure the implementation of appropriate controls to protect against viruses, malware, and ransomware attacks on servers and other IT systems. These measures may include host, network, and application-based intrusion detection and prevention systems (IDS & IPS), customized kernels for Linux, and anti-virus and anti-malware software, among other security measures. Furthermore, updates to anti-virus definition files and automatic system scans shall be conducted regularly to ensure ongoing system security	Network Security Policy and Evidence of Compliance (e.g. endpoint detection and prevention solutions. etc.)	Tier 1&2
CM-NSG.S2	CM-NSG: Network Security (General)	[B] 1. All Service Providers shall establish baseline technical security controls to ensure the uniform application of security configurations across network operations. The minimum security controls include but not limited to: a. Authentication and Authorization: Implement secure authentication and authorization mechanisms (e.g., RADIUS, TACACS+) to control access to network equipment and services. b. Encryption: Use encryption (e.g., AES, IPsec) to protect data in transit, in use and at rest. c. Firewalls and Access Controls: Implement firewalls and access controls (e.g., ACLs, VLANs) to restrict unauthorized access to network equipment and services. d. Intrusion Detection and Prevention: Implement intrusion detection and prevention systems (IDPS) to detect and prevent unauthorized access and malicious activity. e. Implement Zero Trust Architecture: Assume no device or user is	Network Security Policy, Statement of compliance indicating compliance with the minimum security controls.	Tier 1&2

		inherently trustworthy. Enforce strict access controls, continuous authentication, and strict verification for every access request, regardless of location. f. Regular Security Audits and Penetration Testing: Perform regular security audits and penetration testing to identify and remediate security vulnerabilities. g. Security Information and Event Management (SIEM): Implement a SIEM system to collect, monitor, and analyse security-related data from various sources. h. Compliance with Regulatory Requirements: Ensure compliance with relevant policy, statutory and regulatory requirements (e.g., NDPA, Cybercrime Act, NCPS) and industry standards (e.g., PCI-DSS, ISO 27001, ISO 27002 etc). [B] Service Providers shall conduct regular compliance checks to verify that these standards are consistently maintained.		
CM-NSG.S3	CM-NSG: Network Security (General	Service Providers shall establish technical security controls to secure previous and current generations of mobile technology across the network technology stack: 1. Core Network Layer: Service Providers shall secure critical switching infrastructure and backbone services to ensure resilience, confidentiality, and integrity. Including but not limited to: a. Packet-Switched Networks (e.g., IP Core) • Control Plane Protection: Implement control plane policing and filtering to defend against DDoS and route hijacking. • Secure Routing Protocols: Use BGP with RPKI, OSPF authentication, and route validation mechanisms. • Data Plane Security: Deploy IPsec VPNs or MACsec for inter-site data confidentiality and integrity. • Segmentation: Implement VRFs or network slicing to isolate services and customers. b. Circuit-Switched Networks (e.g., Legacy PSTN/SS7) • Signalling Firewall: Deploy SS7/Diameter firewalls with anomaly	Network Operations Policy, Statement of compliance indicating compliance with the minimum technical security controls	UASL (MNO)

		detection and signalling control. • Authentication & Encryption: Use TLS/SIGTRAN for signalling transport; phase out insecure legacy protocols where possible. • Logical Access Control: Limit signalling interface access with firewall zones and ACLs. c. Switching Centers (MSC, GGSN, SGW, etc.) • Zero Trust Architecture: Apply strict identity-based access controls and enforce least privilege. • Centralized Authentication: Use RADIUS or TACACS+ integrated with LDAP/Active Directory. • Audit & Logging: Enable full audit trails, log management with SIEM integration, and regular log reviews. 2. Transmission and IP Layer: Safeguard the network transport infrastructure and IP/MPLS core components against interception, manipulation, and threats to availability a. Transmission Networks (Optical, SDH, Microwave) • Physical Protection: Harden sites with tamper-proof enclosures, access control systems, and video surveillance. • Data Encryption: Apply AES-256 or MACsec over fiber or microwave links. • Failover Design: Implement path redundancy and automatic protection switching (APS). b. IP/MPLS Backbone • Control & Management Plane Isolation: Use out-of-band management and VRFs for segregation. • Label-Switched Path Protection: Enforce LSP integrity with label validation and LDP authentication. • DDoS Protection: Deploy anti-DDoS appliances, flow analysis, and rate-limiting on edge routers. c. Network Equipment (Routers, Switches) • Secure Configuration Baselines: Enforce hardening guides (CIS/NIST) and automate config compliance. • Remote Management Security: Require SSHv2, SNMPv3, and disable		
--	--	---	--	--

		unused services (e.g., Telnet, FTP). • Firmware Integrity: Implement signed firmware updates and supply chain vetting. 3. Access Layer: Defend last-mile access interfaces, radio infrastructure, and edge nodes. a. Radio Access Networks (RAN: 2G/3G/4G/5G) • Air Interface Encryption: Enforce integrity protection and encryption algorithms (e.g., 128-EEA3, 256-NEA2) in 4G/5G. • Baseband Security: Secure O-RAN and DU/CU elements using secure boot, TPMs, and zero-trust onboarding. • Interoperability Controls: Use ETSI TS 33.501 and 3GPP standards for 5G security. b. BTS, eNodeB, gNodeB • Physical Hardening: Install in locked enclosures with intrusion detection, tamper alarms, and UPS systems. • Remote Access Control: Enforce multi-factor authentication (MFA) and jump server access for field engineers. • Patch Management: Automate updates via centralized management systems with secure delivery (e.g., SFTP, OTA). 4. Management & Orchestration (MANO/NMS): Protect administrative interfaces and orchestration systems from unauthorized access and manipulation. a. Configuration Management • Version Control: Use secure configuration repositories (e.g., GitOps with RBAC). • Change Approval: Integrate ITIL change management workflows and multi-party approval. • Encryption & Signing: Protect configs in transit and at rest using TLS 1.3, PKI, and digital signatures. b. Monitoring, Analytics, and Telemetry • Telemetry Security: Transmit metrics via gRPC over TLS, NETCONF over SSH, or RESTCONF over HTTPS. • Centralized SIEM: Correlate events from all layers into a Security		
--	--	---	--	--

		Information and Event Management (SIEM) platform. • Anomaly Detection: Apply machine learning-based behaviour analysis to detect insider threats or APTs. [B] c. Identity & Access Management (IAM) • Role-Based Access Control (RBAC): Enforce granular roles across OSS/BSS and network domains. • Federated Identity: Implement SAML/OpenID Connect for cross-domain identity assurance. • Session Monitoring: Use session recording and time-based access policies for critical systems.		
CM-NSG.S4; CM-NSG.S5	CM-NSG: Network Security (General	[F] 1. Service Providers shall develop a realistic transition strategy toward migrating to IPv6. Such strategy must be approved and at the minimum must contain the following: • compatibility and upgrade strategy for network devices, software, and applications • security measures to protect the IPv6 network from threats. • DNS records update approach to include IPv6 addresses. • Training plan for network engineers and users • Detailed documentation of the IPv6 network configuration and procedures • Monitoring and maintenance procedures to ensure the ongoing performance and security of the IPv6 network. 2. Service Providers shall implement measures to comply with RFC 8200 - Internet Protocol, Version 6 (IPv6) Specification	Transition Strategy Plan	Tier 1&2
CM-NSG.S6	CM-NSG: Network Security (General	[F] Service Providers shall comply with relevant international standards as appropriate 1. BC-004 (Information Security Management) with ISO/IEC 27001/2/11. 2. BC-008 (BCM) with ISO/IEC 22301. 3. BC-011 and BC- 010 (Supply Chain) with ISO/TC 28000. 4. BC-012 (Media Sanitization) with ISO 27040 or NIST SP 800-88. 5. GSM Association Official Document FS.31	Compliance certificate	Tier 1&2

CM: NSCI - Network Security (Critical Infrastructure)				
CM-NSCI.S1	CM-NSCI: Network Security (Critical Infrastructure)	[B] Service Providers shall implement ZTA-aligned controls that are documented in the respective cyber security policies.	Cybersecurity Framework/Policies ISO 27400; ISO 27001/2	Tier 1&2
CM-NSCI.S2	CM-NSCI: Network Security (Critical Infrastructure)	[B] 1. For the development of all software, applications, and feature enhancements, Service Providers shall ensure the establishment of separate production and non-production (test environments). Following development and/or feature enhancements, Software Integration Tests (SIT) shall be conducted to verify that the entire software or application functions as intended. [B] 2. During the development phase of any software or application intended for use by Service Providers or their customers, it must be ensured that vulnerabilities identified by established best practices, such as OWASP guidelines or the top 25 software security vulnerabilities from SANS, are addressed. It is recommended that Service Providers adopt secure development methodologies, such as DevSecOps, to enhance the security of their applications and software.	ISO/IEC 27001 and ISO/IEC 27034	Tier 1&2
CM-NSCI.S3	CM-NSCI: Network Security (Critical Infrastructure)	[B] Access Controls, Password Policy/ Authentication Mechanism 1. No individual, regardless of rank or position, shall have an inherent right to access confidential data, applications, system resources, or facilities. Access shall be granted strictly based on defined roles, responsibilities, and approved authorization protocols. 2. Access to Service Providers' systems, applications, networks, databases, and other resources shall be granted only for a specified purpose and a defined period. Access to IT systems, applications, databases, and networks shall be on a need-to-know basis, adhering to the principle of least privilege. Such access shall be provided for a limited duration and secured through robust authentication mechanisms 3. User access rights, delegated access, unused tokens, and the activities of privileged users shall be reviewed regularly on a periodic basis. 4. Access to external cloud services such as Dropbox, Google Drive,	Information security policy ISO 27001 Network Security Policy ISO 27001 Network Security Policy	Tier 1&2

		iCloud, OneDrive, and similar platforms shall be governed by the Service Providers defined policy and granted only in accordance with approved guidelines 5. Service Providers shall ensure that user access to critical systems is uniquely identifiable and properly logged whenever feasible, to facilitate auditing and review. These logs shall be securely stored for a minimum of two (2) years. Additionally, Service Providers must keep records of users accessing shared accounts. 6. Service Providers shall implement account access lock policies after failure attempts 7. Service Providers shall ensure that regular reviews of existing user accounts and access rights are conducted to identify dormant accounts, accounts with excessive privileges, unknown accounts, or any discrepancies. 8. Service Providers shall ensure that appropriate 'end of life' procedures are implemented for user management, including deactivating access privileges for users leaving the organization or whose access has been revoked. This applies to named user IDs, default user IDs, and generic email IDs. 9. Service Providers shall ensure that all critical systems accessible via the internet are protected with multi-factor security measures, such as VPNs, firewall controls, and multi-factor authentication (MFA). 10. Service Providers shall ensure that multi-factor authentication (MFA) is enabled for all users and systems accessing via online or internet connectivity, with particular emphasis on VPNs, webmail, and accounts that access critical systems from non-trusted environments to trusted environments. [B] Access Controls, Password Policy/ Authentication Mechanism 1. A Privileged Identity Management (PIM) solution or equivalent process shall be implemented to monitor, manage, and audit privileged access across systems and applications. 2. Service Providers shall establish and enforce an access control policy that includes strong password requirements for user access to systems, applications, networks, databases, and other IT resources. Illustrative		
--	--	--	--	--

		examples and guidelines are provided in Annexure-G 3. Service Providers shall develop an Internet access policy to oversee and control the use of internet services, including social media platforms, cloud-based storage, and other related services within the critical IT infrastructure. 4. Service Providers shall implement controls and security measures to monitor staff with elevated system access privileges, such as administrative or privileged users. These measures shall include, but are not limited to, restricting the number of privileged users, conducting periodic reviews of their activities, preventing privileged users from accessing system logs that record their actions, and establishing strong controls over remote access by privileged users.		
CM-NSCI.S4; CM-NSCI.S5; CM-NSCI.S6	CM-NSCI: Network Security (Critical Infrastructure)	[B] Service Providers shall establish technical security controls to secure previous and current generations of mobile technology across the network technology stack: 1. Core Network Layer: Service Providers shall secure critical switching infrastructure and backbone services to ensure resilience, confidentiality, and integrity. Including but not limited to: a. Packet-Switched Networks (e.g., IP Core) • Control Plane Protection: Implement control plane policing and filtering to defend against DDoS and route hijacking. • Secure Routing Protocols: Use BGP with RPKI, OSPF authentication, and route validation mechanisms. • Data Plane Security: Deploy IPsec VPNs or MACsec for inter-site data confidentiality and integrity. • Segmentation: Implement VRFs or network slicing to isolate services and customers. b. Circuit-Switched Networks (e.g., Legacy PSTN/SS7) • Signalling Firewall: Deploy SS7/Diameter firewalls with anomaly detection and signalling control. • Authentication & Encryption: Use TLS/SIGTRAN for signalling transport; phase out insecure legacy protocols where possible. • Logical Access Control: Limit signalling interface access with firewall	Network Operations Policy, Statement of compliance indicating compliance with the minimum technical security controls	UASL (MNO)

		zones and ACLs. c. Switching Centers (MSC, GGSN, SGW, etc.) • Zero Trust Architecture: Apply strict identity-based access controls and enforce least privilege. • Centralized Authentication: Use RADIUS or TACACS+ integrated with LDAP/Active Directory. • Audit & Logging: Enable full audit trails, log management with SIEM integration, and regular log reviews. 2. Transmission and IP Layer: Safeguard the network transport infrastructure and IP/MPLS core components against interception, manipulation, and threats to availability a. Transmission Networks (Optical, SDH, Microwave) • Physical Protection: Harden sites with tamper-proof enclosures, access control systems, and video surveillance. • Data Encryption: Apply AES-256 or MACsec over fiber or microwave links. • Failover Design: Implement path redundancy and automatic protection switching (APS). b. IP/MPLS Backbone • Control & Management Plane Isolation: Use out-of-band management and VRFs for segregation. • Label-Switched Path Protection: Enforce LSP integrity with label validation and LDP authentication. • DDoS Protection: Deploy anti-DDoS appliances, flow analysis, and rate-limiting on edge routers. c. Network Equipment (Routers, Switches) • Secure Configuration Baselines: Enforce hardening guides (CIS/NIST) and automate config compliance. • Remote Management Security: Require SSHv2, SNMPv3, and disable unused services (e.g., Telnet, FTP). • Firmware Integrity: Implement signed firmware updates and supply chain vetting. 3. Access Layer: Defend last-mile access interfaces, radio infrastructure,		
--	--	---	--	--

		and edge nodes. a. Radio Access Networks (RAN: 2G/3G/4G/5G) • Air Interface Encryption: Enforce integrity protection and encryption algorithms (e.g., 128-EEA3, 256-NEA2) in 4G/5G. • Baseband Security: Secure O-RAN and DU/CU elements using secure boot, TPMs, and zero-trust onboarding. • Interoperability Controls: Use ETSI TS 33.501 and 3GPP standards for 5G security. b. BTS, eNodeB, gNodeB • Physical Hardening: Install in locked enclosures with intrusion detection, tamper alarms, and UPS systems. • Remote Access Control: Enforce multi-factor authentication (MFA) and jump server access for field engineers. • Patch Management: Automate updates via centralized management systems with secure delivery (e.g., SFTP, OTA). 4. Management & Orchestration (MANO/NMS): Protect administrative interfaces and orchestration systems from unauthorized access and manipulation. a. Configuration Management • Version Control: Use secure configuration repositories (e.g., GitOps with RBAC). • Change Approval: Integrate ITIL change management workflows and multi-party approval. • Encryption & Signing: Protect configs in transit and at rest using TLS 1.3, PKI, and digital signatures. b. Monitoring, Analytics, and Telemetry • Telemetry Security: Transmit metrics via gRPC over TLS, NETCONF over SSH, or RESTCONF over HTTPS. • Centralized SIEM: Correlate events from all layers into a Security Information and Event Management (SIEM) platform. • Anomaly Detection: Apply machine learning-based behaviour analysis to detect insider threats or APTs. c. Identity & Access Management (IAM)		
--	--	---	--	--

		• Role-Based Access Control (RBAC): Enforce granular roles across OSS/BSS and network domains. • Federated Identity: Implement SAML/OpenID Connect for cross-domain identity assurance. • Session Monitoring: Use session recording and time-based access policies for critical systems.		
CM-NSCI.S7	CM-NSCI: Network Security (Critical Infrastructure)	[B] Service Providers shall implement mutual authentication with appropriate public key infrastructure	Valid Certificates from approved Certification Authorities, X.500/509, ISO 9594-8	Tier 1&2
CM-NSCI.S8	CM-NSCI: Network Security (Critical Infrastructure)	[B] Service Providers shall implement security practices and principles that illustrate Multi Factor Authentication (MFA) in securing Critical Information Infrastructure Assets	Access Control Policy	Tier 1&2
CM-NSCI.S9	CM-NSCI: Network Security (Critical Infrastructure)	[B] The Service Provider shall implement micro segmentation and isolation measures to achieve tenant and container security.	Network Operations Policy	Tier 1&2
CM-NSCI.S10	CM-NSCI: Network Security (Critical Infrastructure)	[F] Service Providers should implement appropriate ML/AI for anomalous detection while documenting limitations and safeguards.	ISO 42001, AI Governance Framework, Network Security Policy	Tier 1&2
CM-NSCI.S11	CM-NSCI: Network Security (Critical Infrastructure)	[B] 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 NCC-CSIRT	CS-ISAC Membership.	Tier 1&2
CM-NSCI.S12	CM-NSCI: Network Security (Critical Infrastructure)	[F] Service providers should implement an automated continuous monitoring capability to validate security configurations, detect configurations drift and anomalies, and generate timely alerts for unauthorized or high-risk changes. Where appropriate, Machine Learning (ML) and Artificial Intelligence (AI) should be used to enhance threat detection, anomalous identification, and security monitoring, while ensuring appropriate governance and periodic validation of AI/ML models.	ISO 42001, AI Governance Framework,	Tier 1&2

CM: PS - Personnel Security

CM-PS.S1	CM-PS: Personnel Security	[B] 1. Service Providers shall ensure that individuals in positions of responsibility within organizations are trustworthy and comply with established security criteria for those roles. [B] 2. Service Providers shall ensure that individuals handling sensitive organizational information and systems are screened prior to being granted access to such information and systems.	Human Resource Policy e.g. Inclusion of background checks for critical roles	Tier 1&2
CM-PS.S2	CM-PS: Personnel Security	[B] 1. Service Providers shall ensure strict compliance with information security policies, access policy and other cybersecurity policies mitigating the risk of intentional harm caused by personnel or other individuals [B] 2. Service Providers shall deploy Endpoint Privilege Management (EPM) to manage risks of intentional harm caused by personnel or other individuals	Information Security policy and evidence of compliance. Subscriptions to relevant EPM solutions	Tier 1&2

CM: ES - Endpoint Security

CM-ES.S1	CM-ES: Endpoint Security	[B] Service Providers shall deploy solutions such as EPP, EDR, XDR, MDR, IPS and anti-malware software to detect threats and attacks on endpoint devices and facilitate rapid response. Additionally, Service Providers must ensure that threat signatures are regularly updated across all IT systems.	Evidence of subscription to Endpoint security solutions (EPP, EDR, XDR, MDR, NG-IPS)	Tiers 1 & 2
CM-ES.S2	CM-ES: Endpoint Security	[B] 1. PowerShell and local administrator rights shall be disabled by default on endpoint machines and shall only be enabled for specific purposes and limited durations. [B] 2. Implement Application Whitelisting solutions to prevent unauthorized execution of PowerShell scripts by default, allowing only approved applications and scripts to run	Information Security Policy, Compliance report on Admin and privileged access rights)	Tier 1&2
CM-ES.S3; CM-ES.S4	CM-ES: Endpoint Security	[I] Service Providers shall subscribe to DNSSEC initiatives and programmes at sectoral and national levels	Compliance report	Tier 1&2

CM: CH - Cyber Hygiene

CM-CH.S1; CM-CH.S2	CM-CH: Cyber Hygiene	[B] The Service Providers shall identify and prioritise critical organisational services, products and their supporting assets.	Risk Management Framework	Tier 1&2
CM-CH.S3	CM-CH: Cyber Hygiene	[B] The Service Providers shall establish an incident response plan and report cyber incidents to the sectoral supervising authorities NCC CSIRT.	Incident Management Framework	Tier 1&2
CM-CH.S4	CM-CH: Cyber Hygiene	[B] The Service Providers shall conduct cybersecurity education and awareness activities for management and staff of the organisation.	Cybersecurity awareness training plan Report of programme/trainings conducted	Tier 1&2
CM-CH.S5	CM-CH: Cyber Hygiene	[B] The Service Providers shall appoint the head of information security/cybersecurity in the organisation with responsibilities and authority for cybersecurity	Confirmation from NCC of CISO appointment	Tier 1&2
CM-CH.S6	CM-CH: Cyber Hygiene	[B] The Service Providers shall comply with all relevant laws, regulations and frameworks in the country	Compliance statement	Tier 1&2
CM-CH.S7	CM-CH: Cyber Hygiene	[B] The Service Providers shall establish adequate network security and monitoring	Network Security Policy	Tier 1&2
CM-CH.S8	CM-CH: Cyber Hygiene	[B] The Service Providers shall control access based on least privilege and maintain the user access accounts consistent with the cybersecurity goal of the organisation	Access Control Policy	Tier 1&2
CM-CH.S9	CM-CH: Cyber Hygiene	[B] The Service Providers shall manage technology changes and use standardised secure configurations including patching and following cyber supply chain risk management standard practices	Change Management Register e.g. Change Register, Change log	Tier 1&2
CM-CH.S10	CM-CH: Cyber Hygiene	[B] The Service Providers shall implement controls to protect and recover data	Data Security Policy	Tier 1&2
CM-CH.S11	CM-CH: Cyber Hygiene	[B] The Service Providers shall prevent and monitor malware exposures	Information Security Policy	Tier 1&2
CM-CH.S12	CM-CH: Cyber Hygiene	[B] The Service Providers shall manage cyber risks associated with suppliers and external dependencies	Supply Chain Policy/ Procurement Policy	Tier 1&2
CM-CH.S13	CM-CH: Cyber Hygiene	[B] The Service Providers shall perform cyber threat and vulnerability monitoring and remediation	Information Security Policy	Tier 1&2

CM-CH.S14	CM-CH: Cyber Hygiene	[B] The Service Providers shall participate in cybersecurity stakeholders' activities to inform, collaborate, share and advance cybersecurity services within the communications sector	Evidence of Compliance e.g. email, letters of invitation, certificate of participation, MOUs etc.	Tier 1&2
CM: CIR - Communication Infrastructure Resilience				
CM-CIR.S1	CM-CIR: Communication Infrastructure Resilience	[B] Service Providers shall conduct comprehensive, scenario-based cyber resilience testing at least twice a year (every six months) to validate their ability to recover and resume operations following a cybersecurity incident or attack within the prescribed RTO and RPO defined by NCC. In this process, Service Providers shall incorporate extreme plausible cyber-attack scenarios into their cyber response and recovery plans. These scenarios may be developed by Service Providers in consultation with their respective IT Security Committees, drawing on insights from sources such as past cybersecurity incidents, near-miss analyses, Security Operations Centre data, honeypot logs, and other relevant information.	Cyber Resilience Testing Report	Tiers 1 & 2
CM-CIR.S2	CM-CIR: Communication Infrastructure Resilience	[B] The Service Providers shall identify, contain and isolate compromised assets to limit damage from adversity.	Incident Handling Report	Tier 1&2
CM-CIR.S3	CM-CIR: Communication Infrastructure Resilience	[B] Service Providers shall conduct periodic backup testing and restoration activities in order to meet RPO & RTO objectives, verifying its usability and integrity	Disaster Recovery Test Report	Tier 1&2
CM-CIR.S4	CM-CIR: Communication Infrastructure Resilience	[B] Service Providers shall align their resilience strategy with the industry cybersecurity resilience best practices and standards	Audit Report	Tier 1&2

CM-CIR.S5; CM-CIR.S6	CM-CIR: Communication Infrastructure Resilience	[F] Service Providers shall implement methodologies and metrics to identify critical functions, systems, and assets that should be prioritized for investments aimed at enhancing resilience of critical infrastructures	Business Impact Analysis Report	Tier 1&2
CM-CIR.S7	CM-CIR: Communication Infrastructure Resilience	[B] 1. The Service Providers shall have a comprehensive understanding of how disruptions can impact critical infrastructure assets, including the identification of dependencies and interdependencies that could amplify their effects. [B] 2. The Service Providers shall implement a whole-of-society approach to critical infrastructure resilience. This governance framework will involve collaboration with ministries, agencies, critical infrastructure owners and civil societies responsible for critical infrastructure delivery and resilience.	Critical infrastructure resilience framework	Tier 1&2
CM-CIR.S8; CM-CIR.S9; CM-CIR.S10	CM-CIR: Communication Infrastructure Resilience	[B] Service providers shall integrate resilience requirements throughout the infrastructure lifecycle by implementing risk-based infrastructure resilient design principles, eliminating single points of failure where practicable, establish effective business continuity and maintain appropriate redundancy and disaster recovery arrangements.	Critical Infrastructure resilience framework (Include a BCP)	Tier 1&2
CM-CIR.S10	CM-CIR: Communication Infrastructure Resilience	Service providers shall develop a risk-based and layered approach by overseeing the implementation process, assessing progress toward resilience objectives, and establishing an accountability framework for critical infrastructure.	Critical Infrastructure resilience framework	Tier 1&2
CM-CIR.S11	CM-CIR: Communication Infrastructure Resilience	[F] Service providers shall support international cooperation to strengthen the resilience of critical infrastructure against cyber and operational threats. This includes participating, where appropriate, in international cybersecurity and resilience initiatives, information-sharing networks, standards development activities, capacity-building programmes, and cross-border incident response and coordination efforts	MOUs, Partnership Agreements	Tier 1&2
CM-CIR.S12	CM-CIR: Communication Infrastructure Resilience	[B] 1. Service Providers shall log the assignment of CNII IP addresses to devices and users. [B] 2. Service Providers shall review and audit CNII IP address assignments and usage biannually to identify unused or stale IP addresses	Biannual CNII IP assignment registers and logs	Tier 1&2

		that could potentially be exploited by malicious actors [B] 3. Service Providers shall monitor and review CNII IP address allocations and actual usage biannually to prevent conflicts, which could lead to network disruptions and degraded performance. [B] 4. Service Providers shall log CNII IP address usage for the purposes of investigating security breaches and other incidents. [B] 5. Service Providers shall log CNII IP address usage for accountability and compliance with legal and regulatory obligations. [B] 6. Service Providers shall regularly review and analyse CNII IP address logs biannually to detect potential security threats, compliance violations, or network management concerns.		
CM: ED - External Dependencies/Supply Chain/Procurement				
CM-ED.S1; CM-ED.S4	CM-ED: External Dependencies/Supply Chain/Procurement	[F] The Service Providers shall have a procurement strategy that has adequate cybersecurity requirements including but not limited to the following provisions: • third party due diligence; • third-party audit; • relevant cybersecurity certifications; • notification of security incidents or vulnerabilities in their assets etc.	Supply chain framework	Tier 1&2
CM-ED.S2	CM-ED: External Dependencies/Supply Chain/Procurement	[B] Service Provider shall Implement relevant cloud security measures (config, segmentation, data residency) to mitigate the risks arising from external dependencies on cloud infrastructure providers.	ISO 27017, CIS Controls v8.x ISO 27001, Supply Chain Risk Management Policy.	Tier 1&2
CM-ED.S3; CM-ED.S5; CM-ED.S6	CM-ED: External Dependencies/Supply Chain/Procurement	[B] The Service Providers shall have relevant industry certifications like ISO/IEC 27017, ISO/IEC 28000, and ISO 27001/2	Valid ISO certifications, NCC type approval certificates	Tiers 1 & 2
CM-ED.S11	CM-ED: External Dependencies/Supply Chain/Procurement	[F] The Service Providers shall develop a supply chain framework that requires pre-procurement and due diligence checks.	Supply chain framework	Tiers 1 & 2

CM-ED.S6; CM-ED.S7	CM-ED: External Dependencies/Supply Chain/Procurement	[I] 1. The Service Providers shall provide ISO 27001/2 and ISO 22301 statements of compliance to improve information security management and business continuity of their suppliers, respectively. [I] 2. The Service Providers shall comply with all local supply chain security compliance issued by NCC as it relates to suppliers of critical infrastructure components	Valid ISO certifications of the third party	Tiers 1 & 2
CM-ED.S8; CM-ED.S9	CM-ED: External Dependencies/Supply Chain/Procurement	[I] 1. The Service Providers shall ensure that third party providers e.g. MSPs, MSSP demonstrate robust internal controls (and effectiveness of the controls) for all services provided under the scope of the service agreement or local regulation compliance. [I] 2. The Service Providers shall provide ISO 9001 and ISO 27001 statements of compliance	Valid ISO certifications of the third party	Tiers 1 & 2
CM-ED.S12	CM-ED: External Dependencies/Supply Chain/Procurement	[B] Service Providers shall provide data and cyber security breach notifications reports when the third party is breached in line with the specified timelines in the CRF NCS.	Breach Notification Report	Tier 1&2
CM-ED.S13	CM-ED: External Dependencies/Supply Chain/Procurement	[B] Service Providers shall ensure that software/firmware packages are signed, and secure delivery mechanisms for hardware and software exist as part of their procurement strategy.	OEM Attestation, Supply Chain Framework/Policy	Tiers 1 & 2
CM-ED.S14	CM-ED: External Dependencies/Supply Chain/Procurement	[B] Service Providers shall define and implement a risk-based patch management (e.g. deployment) policy.	Supply chain framework	Tiers 1 & 2
CM: MR – Maintenance & Repairs				
CM-MR.S1	CM-MR: Maintenance & Repairs	[B] Service Providers shall establish a comprehensive maintenance and repair framework that incorporates the specific requirements for physically security of enterprise resources.	Maintenance & Repair Access logs	Tier 1&2
CM-MR.S2	CM-MR: Maintenance & Repairs	[B] 1. Service Providers shall ensure that only trusted client machines are allowed to access enterprise IT resources remotely. They shall implement appropriate security controls, such as (but not limited to) host integrity checks, binding the MAC address of the device with its IP address, and other	Remote Access Policy/ Framework	Tier 1&2

		relevant measures for remote access and telecommuting. [B] 2. Service Providers shall ensure that suitable risk mitigation measures are implemented whenever third-party service providers are granted remote access to data centre resources. [B] 3. Service Providers shall ensure ongoing monitoring of remote access for any abnormal or unauthorized activities and shall establish mechanisms to generate alerts and alarms to detect and address potential breaches promptly, preventing any damage.		
CM-MR.S3; CM-MR.S6	CM-MR: Maintenance & Repairs	[B] 1. Service Providers shall develop and ensure compliance with patch management procedures which encompasses the identification, categorization, and prioritization of patches and updates. Additionally, a specific timeframe for implementing each category of patches shall be established to ensure timely application. [B] 2. Service Providers shall ensure that all operating systems and applications shall be regularly updated with the latest patches. As an interim measure for zero-day vulnerabilities, and when patches are not immediately available, critical assets shall be isolated to contain the risk until an official patch/update is available. [B] 3. Service Providers shall conduct thorough and rigorous testing of security patches and updates, whenever feasible, prior to deploying them into the production environment. This is to ensure that the application of patches does not adversely affect other systems. [B] 4. Service Providers shall ensure that all patches shall be first tested in a non-production environment that replicates the production environment. [F] 5. Service Providers shall ensure that hardware and software for critical systems shall be replaced prior to reaching their End-of-Life or End-of-Support status. [B] 6. Service Providers shall ensure compensatory controls, such as virtual patching, segmentation, etc. for legacy systems for a maximum duration of 6 months. Additionally, the reasons and constraints necessitating virtual patching must be legitimate and properly documented. [I] 7. Service Providers shall ensure that the procurement of	Patch Management Policy and/or Cybersecurity Framework, Change Management Report	Tier 1&2

		hardware/software shall be aligned with their technology refresh policy. [B] 8. Service Providers shall develop a patch management policy to ensure that all relevant patches for both the Primary Disaster Centre (PDC) and Disaster Recovery (DR) sites are identified, assessed, tested, and applied to all IT systems and applications in a timely manner. This policy shall be approved by the IT Committee of the Service Providers. Furthermore, the IT Committee shall review the patch management policy at least twice a year to ensure its continued effectiveness. [B] 9. Service Providers shall ensure that after the application of any patch or update, the deployed resources are sufficient to deliver the expected level of performance. [B] 10. Service Providers shall establish processes for monitoring patch compliance across all IT systems and applications and regularly report these findings to their respective IT Committee on a quarterly basis.		
CM-MR.S4	CM-MR: Maintenance & Repairs	[B] Depending on the criticality of the patches, Service Providers shall ensure that patches are implemented at both the PDC and DR sites within the maximum timeframes specified in the IT Policy. In cases of emergency patching, patches shall be deployed within the timelines established by the OEMs and provisions for emergency roll back activities.		Tier 1&2
CM-MR.S5	CM-MR: Maintenance & Repairs	[B] Service providers should maintain a documented hardware lifecycle policy that defines requirements for the procurement, deployment, maintenance, upgrade, replacement, and secure disposal of hardware assets. The policy should ensure that hardware remains supported, secure, and resilient throughout its operational lifecycle.	Hardware Asset Register/Inventory	Tier 1&2

PILLAR 4: CYBERSECURITY INCIDENT RESPONSE, MANAGEMENT AND RESILIENCE (GUIDANCE NOTES)

CIRMR: IRP - Incident Response Plan

CIRMR-IRP.S1; CIRMR-IRP.S2; CIRMR-IRP.S3; CIRMR-IRP.S4	CIRMR-IRP: Incidence Response Plan	[B] 1. All Service Providers shall develop an Incident Response Plan as part of their Cybersecurity Crisis Management Plan. These plans shall contain playbooks and use-cases to test the effectiveness of detection processes. [B] 2. The Incident Management plan shall outline the responsibilities and actions to be undertaken by employees and support or outsourced staff in the event of a cyberattack or cybersecurity incident. [B] 3. Service Providers shall develop a Standard Operating Procedure (SOP for handling cybersecurity incident response and recovery for the various cybersecurity attacks. [B] 4. The SOP for reporting of cybersecurity incidents to NCC-CSIRT is contained in the framework (Annexure IV)	An Incident Response Plan An SOP	Tier 1&2
CIRMR-IRP.S5	CIRMR-IRP: Incidence Response Plan	[B] The Service Providers 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).	Cybersecurity Framework and/or ISO 62443, ISO 27001, and other applicable standards	Tiers 1 & 2
CIRMR-IRP.S6; CIRMR-IRP.S7; CIRMR-IRP.S8	CIRMR-IRP: Incidence Response Plan	[B] 1. The Service Providers shall implement appropriate SIEM tools or subscribe to SIEM services to collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack. [B] 2. The Service Providers shall implement detection and prevention tools, XDR, EDR, MDR, and anti-malware tools to automate the rapid response and prevention of malicious code.	SIEM subscription	Tier 1&2

CIRMR: CSM - Continuous Security Monitoring

CIRMR-CSM.S1; CIRMR-CSM.S2; CIRMR-CSM.S3	CIRMR-CSM: Continuous Security Monitoring	[F] 1. The service provider shall establish (or contracts) a Cyber Security Operations Centre (C-SOC) [F] 2. To strengthen security monitoring, Service Providers are required to establish or engage SOC services for managing cybersecurity issues. Service Providers may select from the following models to utilize SOC services: a. Service Providers’ own SOC or Group’s SOC (if Service Providers is part of a group of company) b. A virtual Security Operations Center (vSOC). c. Third party managed SOC provider. [F] 3. The service provider shall engage SOC providers from an NCC approved list of SOC providers.	SOC or SOC-as-a-Service subscription	Tier 1&2
CIRMR-CSM.S4	CIRMR-CSM: Continuous Security Monitoring	[B] 1. Service Providers shall ensure that the utilization of IT assets and resources is continuously monitored and optimized, with projections made for future capacity requirements to ensure the necessary system performance aligns with business objectives. 2. Service Providers shall ensure that IT assets and resources are consistently monitored and fine-tuned, with forecasts developed for future capacity needs to guarantee that system performance effectively supports business objectives: Capacity management shall consist of three main types: a. Data storage capacity – (e.g. in database systems, file storage areas, etc.) b. Processing power capacity – (e.g. adequate computational power to ensure timely processing operations) c. Communications capacity – (“bandwidth” to ensure communications are made in a timely manner). Capacity management shall be; a. Pro-active – for example, using capacity considerations as part of	Capacity utilization report	Tiers 1 & 2

		change management; [I] b. Reactive – e.g. triggers and alerts for when capacity usage is reaching a critical threshold so that timely increments (temporary or permanent) can be made		
CIRMR-CSM.S5	CIRMR-CSM: Continuous Security Monitoring	[B] 1. Service Providers shall perform regular cybersecurity audits and Vulnerability Assessment and Penetration Testing (VAPT) with the scope specified in the CRF NCS to identify vulnerabilities within the IT environment. Additionally, Service Providers shall conduct comprehensive evaluations of the system's security posture through simulations of actual attacks. [B] 2. The Service Providers shall ensure that the assets covered in regular cybersecurity audits shall include (but are not limited to) all critical systems, infrastructure components such as networking systems, security devices, load balancers, servers, databases, applications, remote access points, systems accessible via WAN, LAN, or public IPs, websites, and other IT systems related to operational function. [B] 3. Service Providers shall perform VAPT prior to the commissioning of new systems, especially those which are part of critical systems or connected to critical systems. [I] 4. Revalidation of VAPT after addressing observations shall be conducted within a specified timeframe (as contained in the Cybersecurity Policy) to ensure that all identified vulnerabilities have been effectively remediated. [B] 5. In the event of vulnerabilities found in Commercial Off the Shelf applications (used for core business) or empanelled applications, Service Providers shall promptly report these issues to the respective vendors and the NCC-CSIRT.	Audit and VAPT reports	Tier 1&2

CIRMR: DP - Detection Process

CIRMR-DP.S1; CIRMR-DP.S2	CIRMR-DP: Detection Process	[F] 1. Service Providers shall perform red teaming exercises at least once a year as part of their cybersecurity framework, utilizing red and blue teams to assess and enhance security posture. [F] 2. Service Providers shall implement a Continuous Automated Red Teaming (CART) solution to enable ongoing, automated testing of system security and to enhance visibility into potential attack surfaces. [F] 3. For red teaming exercises, the red team may include Service Providers' employees and/or external experts. [F] 4. The outcomes of the red teaming exercise shall be presented to the IT Committee of the Service Providers and the Management/Board. The lessons learned from these exercises shall be shared, with the IT Committee monitoring the status of remediation efforts for any observations identified during the red team exercise.	Cybersecurity Framework, Red/Blue team exercise reports	Tiers 1 & 2
CIRMR-DP.S3	CIRMR-DP: Detection Process	[B] Threat hunting, utilizing threat intelligence, Indicators of Compromise (IOCs), Indicators of Attacks (IOAs), and other relevant assessments, shall be carried out on a quarterly basis.	Vulnerability & Compromise Assessment Reports	Tiers 1 & 2

CIRMR: CCMP - Incident Management (Cyber Crisis Management Plan)

CIRMR-CCMP.S1	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan)	[B] 1. All Service Providers shall develop an Incident Management Plan as part of their Cybersecurity Crisis Management Plan [B] 2. The SOPs shall outline scenario based responsibilities and actions to be undertaken by employees and support or outsourced staff in the event of a cyberattack or cybersecurity incident.	Cyber Crisis Management Plan (CCMP)	Tier 1&2
CIRMR-CCMP.S2; CIRMR-CCMP.S3; CIRMR-CCMP.S4;	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan)	[B] 1. In order to optimize the Service Providers' ability to respond in a timely and appropriate manner, Service Providers shall: a. Create cybersecurity awareness b. Provide cybersecurity training to the relevant teams, c. Develop/ hire people with appropriate skill-sets, d. Prepare cyber playbooks,	Cybersecurity Framework/Cyber Crisis Management Plan (CCMP), Evidence of SIEM/SOAR service subscription	Tiers 1 & 2

CIRMR-CCMP.S5		e. Utilise relevant SIEM/SOAR tools and services f. Create knowledge database for all known adverse conditions and attacks [B] 2. Service Providers shall develop a Standard Operating Procedure (SOP for handling cybersecurity incident response and recovery for the various cybersecurity attacks approved by leadership of the Service Providers. [B] 3. The SOP for reporting of cybersecurity incidents to NCC-CSIRT is attached at Annexure-IV [B] 4. Service Providers shall ensure that, following a cybersecurity incident (if any), they update their response and recovery plans to strengthen their cyber resilience and incorporate the lessons learned from the incident.		
CIRMR-CCMP.S6; CIRMR-CCMP.S7	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan)	[F] 1. For all incidents classified as High or Critical affecting CNII, Service Providers may be required to submit a forensic audit or investigation report. [F] 2. Upon completion of the forensic audit, Service Providers shall submit a final closure report that includes the root cause of the incident, its impact, and measures to prevent recurrence. The NCC shall determine the timeline for submitting these reports, including the closure report,.	Audit report and/or Closure reports	Tier 1&2
CIRMR-CCMP.S8	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan)	[B] 1. The Service Providers cybersecurity committee shall review and discuss response plans, coordinate with stakeholders to ensure consistency in response actions, facilitate information sharing for improved awareness, and address related matters. [B] 2. To facilitate effective incident response coordination, Service Providers shall regularly update their contact details, intermediaries, and other relevant stakeholders.	Cyber Crisis Management Plan (CCMP)	Tier 1&2
CIRMR-CCMP.S9	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan)	[I] Service Providers shall get onboarded to the NCC CSIRT's VTEM and other CSIRT initiatives	Subscription to NCC CSIRT's VTEM Platforms	Tier 1&2

CIRMR-CCMP.S10	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan))	[B] 1. Any cyber-attack, cybersecurity incident, and/or breach involving a Service Provider's system, network, or critical asset shall be reported to NCC-CSIRT within 4 hours of detection or awareness of the incident. This information shall be shared with NCC-CSIRT via incident@csirt.ncc.gov.ng within the same 4-hour timeline. Additionally, comprehensive details of the incident must be submitted through the NCC-CSIRT Incident Reporting Portal within 24 hours [B] 2. The Service Providers whose systems have been designated as "Critical National Information Infrastructure" by the Presidential Order on the Designation of Critical National Information Infrastructure (CNII) shall additionally report the incident to the NCC through the CNII Industry escalation protocols. [B] 3. Quarterly reports detailing cyber-attacks, threats, cybersecurity incidents, breaches experienced by Service Providers, and the measures taken to mitigate vulnerabilities, threats, and attacks including information on bugs, vulnerabilities, and emerging threats that may be useful to other Service Providers and NCC shall be submitted to NCC-CSIRT within 15 days after the end of each quarter (June, September, December, and March). [B] 4. Such information, considered useful for sharing with other Service Providers in an anonymized or masked form, shall be shared using the mechanisms specified by NCC-CSIRT from time to time. When sharing the sensitive information, the Traffic Light Protocol (TLP) shall be used to indicate four levels of sensitivity: white, green, amber, or red. [B] 5. During the incident investigation process by NCC-CSIRT, Service Providers shall, when necessary, provide regular updates, including reports such as Root Cause Analysis (RCA), forensic analysis reports, and other relevant progress reports on the ongoing incident analysis.	Email trails and logs of ISAC platform	Tier 1&2
CIRMR-CCMP.S11	CIRMR-(CCMP: Incident Management (Cyber Crisis Management Plan))	[I] Service Providers shall utilize Threat Intelligence data, including information collected, processed, and analysed to gain insights into the motives, behaviour of threat actors, targets, attack patterns, and related aspects, through OSINT platforms.	Subscription to OSINT and other related threat intelligence platforms	Tier 1&2

CIRMR: IReP - Incident Recovery Plan (Execution & Communication)				
CIRMR-IReP.S1	CIRMR-IRP: Incident Recovery Plan (Execution & Communication)	[B] 1. Service Providers' response and recovery plans shall incorporate scenario-based classifications. Each Service Provider shall develop their own response and recovery strategies tailored to their specific business model. [B] 2. Service Providers' response and recovery plans shall include strategies for the swift restoration of systems affected by cybersecurity incidents, attacks, or breaches, such as providing alternative services or systems to customers. These plans shall be tested through simulations designed to challenge assumptions related to response, resumption, and recovery practices, including governance structures and communication protocols. The testing process shall involve all relevant stakeholders, such as critical service providers, vendors, linked Service Providers, and others. [I] 3. Service Providers shall regularly keep updated 'golden images' of critical systems stored at an offsite location for system reconstruction whenever necessary. These images or 'templates' shall include a preconfigured operating system (OS), configuration settings, backup data, and associated software applications that can be rapidly deployed to rebuild a system, such as a virtual machine or server. [F] 4. Service Providers shall consider the option of maintaining spare hardware in an isolated environment to facilitate system reconstruction if starting operations from Primary Data Center and/or Disaster Recovery Services is not feasible. They shall also aim to keep spare hardware in a ready-to-use state to ensure the delivery of critical services. These systems shall be updated regularly to incorporate new changes, such as OS patches and security patches, applied to the primary systems. Additionally, the spare hardware shall undergo routine testing in accordance with the Service Provider's response and recovery plans. [I] 5. Service Providers shall exercise all necessary precautions when updating 'golden' server images and data backups to ensure that the server images and backups remain intact and uncorrupted. [B] 6. In the event of ransomware attacks that specifically target backups,	Incident recovery playbooks and scripts highlighting compliance with CRF NCS KPIs	Tier 1&2

		traditional data backups may prove insufficient. Therefore, Service Providers shall create backups in an isolated, immutable, and/or air-gapped manner to ensure effective recovery if the production system is compromised. [F] 7. Service Providers shall conduct regular business continuity drills to evaluate the organization's preparedness and the effectiveness of existing security controls at the operational level. One recommended scenario for testing is recovery from a ransomware attack, assuming both Primary Data Center and/or Disaster Recovery Services have been impacted. This will help assess the effectiveness of personnel, processes, and technologies in responding to and managing such incidents.		
CIRMR-IReP.S2	CIRMR-IRP: Incident Recovery Plan (Execution & Communication)	[B] 1. In the event of a disruption to one or more critical systems, the Service Providers shall, within 30 minutes of the incident, classify it as a 'Disaster' based on the business impact analysis and in line with the NCC Disaster Recovery Guidelines 2023. The targeted recovery time objective (RTO) shall be two (2) hours for the resumption of critical operations, while the recovery point objective (RPO) shall be 15 minutes for all Service Providers. The recovery plan shall be scenario-based and aligned with the specified RTO and RPO. [F] 2. Service Providers shall conduct comprehensive, scenario-based cyber resilience testing at least biannually to validate their ability to recover and resume operations following a cybersecurity incident or attack within the prescribed RTO and RPO as defined by NCC. In this context, Service Providers shall incorporate highly plausible and severe cyber-attack scenarios into their cyber response and recovery plans. These scenarios may be developed by Service Providers in consultation with their respective IT Security Committees, drawing on insights from past cybersecurity incidents, near-miss analyses, data from Security Operations Centers, honeypot logs, and other relevant sources. [B] 3. Service Providers shall regularly perform backup testing by restoring backup data to verify its usability and integrity. [I] 4. For cyber resilience testing, Service Providers shall also involve stakeholders that are critical to the restoration activities of the service	Incident recovery playbooks and scripts highlighting compliance with CRF NCS KPIs Disaster Recovery Plan	Tier 1&2

		provider. 5. The outcomes and lessons learnt of the cyber resilience testing shall be presented to the IT Security Committee of the Service Providers.		
CIRMR-IReP.S3	CIRMR-IRP: Incident Recovery Plan (Execution & Communication)	[I] 1. All Service Providers shall conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan. [I] 2. Service Providers shall conduct regular business continuity drills to evaluate the organization's preparedness and the effectiveness of existing security controls at the operational level.	Incident recovery playbooks and scripts highlighting compliance with CRF NCS KPIs	Tier 1&2
CIRMR-IReP.S4	CIRMR-IRP: Incident Recovery Plan (Execution & Communication)	[B] 1. Service Providers shall develop a backup and recovery plan, which must be approved by their respective IT Security Committees. This plan shall incorporate policies and software solutions designed to ensure business continuity in the event of a security incident. It shall also include clear guidance on data restoration using the backup software employed by the Service Providers. [B] 2. The backup and recovery policy shall encompass both data backups and server image backups. [B] 3. The backup of data and server images shall be maintained at off-site locations to keep backup copies intact and unbroken [B] 4. The recovery plan shall include RTO (Recovery Time Objective) and RPO (Recovery Point Objective), as specified by NCC from time to time, for the restoration of systems following cybersecurity incidents. [I] 5. Service Providers shall maintain offline, encrypted backups of data and conduct regular testing of these backups at least quarterly to verify their confidentiality, integrity, and availability.	DRP/BCP	Tier 1&2
CIRMR-IReP.S5	CIRMR-IRP: Incident Recovery Plan (Execution & Communication)	[B] 1. In the event of a high-impact cyber-attack with a widespread effect (as defined in the cybersecurity framework), the Service Providers shall publish a press release. This release should include, at a minimum, a summary of the incident, details of the recovery actions undertaken, the status of normal operations restored, and other necessary details of affected customers and stakeholders. [B] 2. In the event of a low impact and has a limited or low reach (as	Press release sheets	Tier 1&2

		defined in the cybersecurity framework), the Service Providers shall inform affected customers and stakeholders.		
CIRMR-IReP.S6	CIRMR-IRP: Incident Recovery Plan (Execution & Communication)	[B] The updates and changes in the contingency plan, training exercises, and incident response and recovery plan shall be communicated and approved by the Board/Partners/ Proprietor.	Cyber Crisis Management Plan (CCMP)	Tier 1&2
CIRMR: RM - Resilience Management				
CIRMR-RM.S1	CIRMR-RM: Resilience Management	[B] 1. Service Providers shall strive to reduce their attack surfaces. [B] 2. Service Providers shall actively review controls, practices, and capabilities to identify and prepare for prospective, emerging, or potential threats. [B] 3. Service Providers shall continuously enhance their ability to swiftly deploy and integrate both existing and new services and technologies, whether on-premises or in the cloud. [I] 4. Service Providers may proactively identify potential new attack vectors through threat modelling based on risk assessments and implement measures to defend against them.	Vulnerability & Threat Exposure Management Systems (VTEM) Report, Risk Assessment Report	Tiers 1 & 2
CIRMR-RM.S2	CIRMR-RM: Resilience Management	[B] Service Providers' architectures shall be designed to eliminate single-points of failure with redundancy, cut-over management and load- balancing.	Cybersecurity Framework/Policy or Cyber resilience Plan	Tier 1&2
CIRMR-RM.S3	CIRMR-RM: Resilience Management	[B] Service Providers shall maintain additional capacity of IT assets for purposes such as information storage, processing, or communications.	Capacity Management Policy	Tier 1&2
CIRMR-RM.S4; CIRMR-RM.S5; CIRMR-RM.S6	CIRMR-RM: Resilience Management	[B] Service Providers shall periodically exercise service-specific documented Business Continuity Management (BCM) and DRP plans.	DRP/BCP, Cyber resilience Plan	Tier 1&2
CIRMR-RM.S7	CIRMR-RM: Resilience Management	[I] 1. Service Providers shall implement different audit and logging regimes across various architectural layers. [I] 2. Service Providers shall evaluate the feasibility of deploying multiple	Cybersecurity Framework/Log Management Policy, Cyber	Tier 1&2

		operating systems, ensuring that an attack or compromise on one type of OS does not affect other deployed OS.	resilience Plan	
CIRMR-RM.S8	CIRMR-RM: Resilience Management	[F] Service Providers shall utilize data analytics to drive decision-making.	Analytics Report/Cyber resilience Plan	Tier 1&2
CIRMR-RM.S9	CIRMR-RM: Resilience Management	[B] Service Providers shall proactively evaluate and implement necessary actions related to their system's requirements, architecture, design, configuration, acquisition processes, and operational procedures as part of their strategy to adapt to identified and emerging threats and vulnerabilities.	Cybersecurity Framework, Cyber resilience Plan	Tier 1&2

**PILLAR 5: CYBERSECURITY CAPACITY BUILDING AND DEVELOPMENT
(GUIDANCE NOTES)**

CCB: CSD - Cybersecurity Skill Development

CCB-CSD.S1; CCB-CSD.S2	(CCB-CSD: Cybersecurity Skill Development	[B] 1. The Service Providers shall focus on fostering awareness of cybersecurity, cyber resilience, and system hygiene among employees, particularly emphasizing those in non-technical roles. The periodicity shall be bi-annually for Service Providers staff. [B] 2. The Service Providers shall ensure that privileged users are knowledgeable about potential risks such as social engineering attacks, phishing, and other security threats. [B] 3. Given that most infections are mainly caused by phishing emails, malicious advertisements on websites, and third-party apps and programs, the Service Providers shall develop well-designed security awareness campaigns emphasizing the importance of avoiding clicking on links and attachments in emails as a key component of the defense strategy. Additionally, advisories issued by NCC-CSIRT may be consulted for guidance and support in conducting public awareness exercises [B] 4. The Service Providers shall ensure that the training programs shall	Employee/Cybersecurity Training plan, Cybersecurity Framework	Tier 1&2
---------------------------	---	--	---	----------

		be periodically reviewed and updated to ensure that their content remains current, accurate, and relevant.		
CCB-CSD.S3	(CCB-CSD: Cybersecurity Skill Development)	[B] 1. The Service Providers shall regularly endeavour to organize training programs to improve third-party stakeholders' understanding of IT and cybersecurity policies and standards, including current cybersecurity threats. Cybersecurity awareness sessions should be carried out for outsourced employees, third-party service providers, and other relevant personnel. [B] 2. In order to optimize the Service Providers' ability to respond in a timely and appropriate manner, Service Providers shall: a. Create cybersecurity awareness b. Provide cybersecurity training to the relevant teams c. Develop/ hire people with appropriate skill sets d. Prepare cyber playbooks,	Employee/Cybersecurity Training plan Cybersecurity Framework	Tier 1&2
CCB-CSD.S4	(CCB-CSD: Cybersecurity Skill Development)	[B] The Service Providers shall work on training and raising awareness of cybersecurity, cyber resilience, and system hygiene among physical and information security personnel.	Employee/Cybersecurity Training plan Cybersecurity Framework	Tier 1&2
CCB: CTA - Cybersecurity Training and Awareness				
CCB-CTA.S1	(CCB-CTA: Cybersecurity Training and Awareness)	[B] The Service Providers shall work on building awareness of cybersecurity, cyber resilience, and system hygiene among employees (with a focus on new employees which should be part of their on-boarding process)	Employee/Cybersecurity Training plan	Tier 1&2
CCB-CTA.S2	(CCB-CTA: Cybersecurity Training and Awareness)	[B] The Service Providers shall develop a dedicated program on cybersecurity governance responsibilities, building awareness of cybersecurity, cyber resilience, and system hygiene for board members and senior executives. The periodicity shall be bi-annually.	Approved cybersecurity training plan	Tier 1&2
CCB-CTA.S3	(CCB-CTA: Cybersecurity Training and Awareness)	[B] The Service Providers shall develop a plan of action to: 1. Improve and maintain customer awareness and education regarding cybersecurity risks. 2. Encourage customers to report phishing mails/ phishing sites to their service providers and on such reporting should be logged and auditable for	Cybersecurity Advocacy reports	Tier 1&2

		effective remedial action 3. Educate customers of communication services about the risks of sharing their login credentials, passwords, OTPs, or similar information with third parties, as well as the potential consequences of such actions.		
CCB: CRD - Cybersecurity Research & Development				
CCB-CRD.S1	(CCB-CRD: Cybersecurity Research & Development	[F] The Service Providers should support cybersecurity research and development through sponsorships, research collaborations, exposure programmes with Nigerian Universities and scholars of cybersecurity research	Research output (Publications, programmes etc)	Tier 1&2
CCB-CRD.S2	(CCB-CRD: Cybersecurity Research & Development	[F] The Service Providers should consciously adopt and participate in Student Industrial Work Experience Scheme (SIWES) programmes for students in cybersecurity related disciplines from Nigerian tertiary institutions.	Reports of accepted SIWES programmes	Tier 1&2
CCB: CECC - Cybersecurity Ecosystem and Cross-Sector				
CCB-CECC.S1	(CCB-CE (CC: Cybersecurity Ecosystem and Cross Sector Cooperation	[B] The Service Providers are encouraged to take part in PPP initiatives to improve cybersecurity posture at sectorial and national levels.	Signed MOU, agreements etc.	Tier 1&2
CCB-CECC.S2	(CCB-CE (CC: Cybersecurity Ecosystem and Cross Sector Cooperation	[B] The Service Providers are encouraged to participate in initiatives related to cybersecurity or collaborate with academic institutions, NGOs, innovation hubs, professional organizations, international development agencies, and others to strengthen the sector's cybersecurity ecosystem	Signed bi-lateral and multi-lateral MOU, agreements etc	Tier 1&2
CCB-CECC.S3	(CCB-CE (CC: Cybersecurity Ecosystem and Cross Sector Cooperation	[B] The 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	Signed evidence of participation.	Tier 1&2