Regulatory Guidelines for Government Information Security Management

ISSUED BY THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA)

Table of Contents

DRAFT

DRAFT

1 Explanatory Note

This Regulatory Guidelines for Government Information Security Management sets out the Nigerian Government's approach to managing information and cyber security. The Guideline is based on a risk management approach and requires Institutions to implement procedures and controls that are proportionate to the level of information and cyber risk they face. The Guideline provides a comprehensive approach to managing information and cyber security risks based on extant statutory and industry frameworks.

These Guidelines impose two complementary and co-existing categories of obligation:

(i) Information Security Governance — the management-system requirements set out in Section 12 (governance, policy, risk management, performance evaluation, internal audit, and improvement); and

(ii) Cybersecurity Technical Controls — the operational and technical controls scheduled in Annex 1.

Full compliance requires conformance with BOTH categories. The governance requirements establish how an FPI directs and assures its programme; the Technical controls establish what protective measures it implements. Where This document refers to "information and cyber security," both categories are engaged. [A4]

2 Authority

In exercise of the powers conferred on it by Sections 6 and 17 of the National Information Technology Development Act of 2007, the National Information Technology Development Agency (NITDA) hereby issues the Regulatory Guidelines for Government Information Security Management.

i. These Guidelines are issued under the authority of the National Information Technology Development Act 2007 (NITDA Act) and constitute a regulatory instrument of NITDA. The Guidelines are complementary to, and operate within, the national cybersecurity governance framework established by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024) and the National Cybersecurity Policy and Strategy (NCPS) 2021.

DRAFT

ii. Under the NCPS 2021, the Office of the National Security Adviser (ONSA) through the National Cybersecurity Coordination Centre (NCCC) is the apex coordinating authority for Nigeria's national cybersecurity programme. NITDA operates as the lead agency for ICT and cybersecurity technology standards across government, interfacing with the NCCC in accordance with NCPS 2021, Section 9.1. These Guidelines are issued in exercise of NITDA's standards and compliance mandate within that framework and do not purport to exercise the coordination and enforcement functions vested in ONSA.

iii. Where any provision of these Guidelines intersects with an obligation under the Cybercrimes Act 2015 (as amended) and NCPS 2021, FPIs shall satisfy both obligations. Where there is a genuine conflict between the instruments, the Cybercrimes Act 2015 (as amended) and NCPS 2021 shall prevail, and NITDA shall seek resolution through inter-agency coordination with ONSA/NCCC.

iv. Criminal offences under the Cybercrimes Act 2015 (as amended) fall within the jurisdiction of the Nigeria Police Force, the Economic and Financial Crimes Commission, and other designated law enforcement agencies. NITDA's enforcement powers under these Guidelines are administrative in nature. Nothing in these Guidelines confers on NITDA criminal investigative or prosecutorial authority.

v. References to the Cybercrimes Act 2015 (as amended) in the Framework Reference column of Annex 1 are provided as alignment and mapping references to indicate where a control addresses obligations under that Act. Such references are informative, not constitutive of NITDA's authority to enforce compliance with the Act itself.

3 Title and Commencement

These Guidelines may be cited as the Regulatory Guidelines for Government Information Security Management and shall come into effect on the date this document is signed.

4 Application

The Guidelines shall apply to all Public Institutions, including Ministries, Commissions, Departments and Agencies at the Federal level. State, Local Government and Private Sector entities are encouraged to adopt the

DRAFT

Guidelines as exemplary practice and tailor it to suit their peculiarities for information security management.

5 Definitions

Asset: anything that has value to the organization
Control: measure that maintains and/or modifies risk
Personnel: persons doing work under the organization's direction
Policy: intentions and direction of an organization, as formally expressed by its top management
Procedure: specified way to carry out an activity or a *process*
Process: set of interrelated or interacting activities that use or transform inputs to deliver a result
Threat: potential cause of an unwanted incident, which can result in harm to a system or org
Information Security: the preservation of confidentiality, integrity, and availability of information. Other properties such as authenticity, accountability, non-repudiation, and reliability can also be part of Information Security.
Information Systems: any computer within an organisation that is used to store and process information and data.
FPI: Federal Public Institutions
Organisation(s): Refers to FPI's, Federal Government-owned corporations, and companies, either fully or partially owned by the Federal Government.
Risk: A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
Risk Assessment: Comprehensive concept for defining and assessing the potential impact of threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information suitable for a (risk management) decision to optimise investment in security countermeasures.
Risk Management: A systematic process of identifying, assessing, and mitigating risks to minimize potential impact and ensure organizational objectives are achieved
Information Security Program: a structured set of policies, processes, and controls designed to protect an organization's information assets and ensure confidentiality, integrity, and availability

DRAFT

Cybersecurity: the protection of information systems, networks, devices, and data from cyber threats through technical and operational controls. Within these Guidelines, Cybersecurity denotes the operational and technical control layer, while Information Security denotes the overarching management system that governs it.

6 Purpose

The Nigerian Government is responsible for a significant amount of information. To ensure trust and deliver business value, it is critical that this information is protected appropriately. This regulatory Guideline seeks to ensure all public institutions in Nigeria apply a consistent, risk-based approach to the implementation of information and cyber security to ensure:

a) Confidentiality of information: making sure that information is accessible only to those authorized to have access.
b) Integrity of information: safeguarding the accuracy and completeness of information and data processing methods.
c) Availability of information: making sure that authorized users have access to information and assets when required.
d) Protection of people: making sure personal information is safe.
e) Continuous improvement: implementation of processes for continuous security assessment, security control assessment, awareness, training, security audit and incident response.

7 Objectives

These Guidelines are issued to achieve the following objectives:

a) Protection and sustenance of an organization's information;
b) Protection of the organization's information assets and strategic processes;
c) Deepening of the organization's information security awareness culture;
d) Strengthening of internal control processes while maintaining external and stakeholders' confidence; and
e) Achieving organizational wide information protection and increasing resilience to unwholesome practices and cyberattacks.
f) Managing information and cyber security risks that can prevent organisations from achieving their statutory mandates.

DRAFT

8 Enforcement

8.1 Enforcement Authority

These Guidelines shall be enforced by the National Information Technology Development Agency (NITDA) in exercise of the powers conferred by Sections 6(a), 6(c), and 17 of the National Information Technology Development Act 2007. NITDA's enforcement role under these Guidelines is administrative and regulatory in nature. Criminal offences disclosed in the course of enforcement shall be referred to the appropriate law enforcement authorities in accordance with the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024).

8.2 Enforcement Instruments

In discharging its enforcement mandate, NITDA may deploy the following instruments:

A. compliance notices requiring specific remedial action within a defined period;
B. surveillance and monitoring of FPIs' information security posture;
C. formal queries and mandatory self-assessment returns;
D. special audits initiated by NITDA or conducted by NITDA-accredited auditors;
E. administrative sanctions in accordance with Section 7.4 of these Guidelines;
F. and Investigative procedures where material non-compliance or deliberate concealment is suspected.

8.3 Compliance Status Classification

NITDA shall classify FPIs' compliance status as follows following audit or assessment:

Classification	Description
Compliant	FPI meets all applicable control requirements for its CMMI stage and risk profile
Partially Compliant	FPI meets core governance and foundational controls but has identified gaps in operational or technical controls
Materially non-compliant	FPI has significant gaps across multiple domains or has failed to remediate findings from a previous audit cycle

DRAFT

Critically non-compliant	FPI has systemic control failures, has experienced a significant incident attributable to non-compliance, or has failed to engage with NITDA's enforcement process

9 Review and Amendment

NITDA shall amend or review these guidelines periodically or as the need arises. Such review or amendment shall be carried out under the NITDA Act 2007 or relevant policy directives of the Federal Government and shall take into consideration the following:

a) changes in government policies and strategic objectives regarding Information and Communications Technology and Digital Economy;
b) an assessment of the effectiveness of these Guidelines in achieving its goals;
c) emerging trends in the global ICT industry and standards that may have significant implications for the achievements of the objectives;
d) emerging global information and cyber security frameworks and code of practice for controls.

10. Breach

A breach of these Guidelines constitutes a breach of the National Information Technology Development Act 2007 and shall be subject to the enforcement regime established under Section 8 of these Guidelines. NITDA shall maintain a penalty register of enforcement actions taken under these Guidelines, which shall form part of NITDA's annual regulatory report to the Federal Government.

11 General Provisions

a) FPIs shall establish, implement, maintain, and continually improve an Information security management program, in accordance with the requirements of this regulation.
b) FPIs shall establish a governance committee for the governance of their Information and Cyber Security programme.

FPI’s shall establish an Information Security Management Team and assign qualified staff as required to administer the organizations information security management program. This Team shall include a Chief Information Security

DRAFT

Officer (CISO), Information Security (IS) Managers, Risk Managers, IS Internal Auditors, IS Implementers, IS Compliance Team. This Team shall also include a Computer Emergency Response Team (CERT) for threat intelligence management, Vulnerability Assessment/Penetration Testing (VAPT) and incident response.

FPIS shall develop and implement an annual Information and Cyber Security Programme Plan. This plan shall include but not limited to risk assessment plan, awareness and training plan, VAPT plan, audit plan, continuous improvement plan.

An FPI may discharge operational security obligations under these Guidelines — including CERT functions, security monitoring, vulnerability management, and incident response — through any of the following models, or a combination thereof:

Internal capability maintained by the FPI;

Shared government security services (for example, through Galaxy Backbone or other centrally provided platforms);

Accredited Managed Security Service Providers (MSSPs); or

Centralised monitoring, detection, and response arrangements operated on behalf of a group of FPIs.

Where a function is shared or outsourced, the FPI shall retain documented accountability, a written service agreement defining security responsibilities, and the right to audit the provider. Adoption of a shared or outsourced model does not transfer the FPI's compliance obligations under these Guidelines. Lower-maturity FPIs (Silo and Engaged stages) are particularly encouraged to adopt shared or outsourced models for resource-intensive functions.

FPIS shall establish an Information and Cyber Security compliance and audit function for regular compliance monitoring and internal auditing of the organization Information and Cyber security management program.

B2: FPIs shall be subjected to a mandatory annual Information and Cyber Security audit conducted by NITDA-accredited Information and Cyber Security Auditors. The following requirements apply:

(i) *Auditor Accreditation*: NITDA shall maintain a public register of accredited auditors eligible to conduct audits under these Guidelines. The criteria, application process, and competency requirements for auditor accreditation are set out in the Cybersecurity Auditor Accreditation Framework issued by NITDA, which operates as a companion instrument to these Guidelines.

DRAFT

FPIs shall only engage auditors listed on NITDA's accredited auditor register.

(ii) *Audit Report Submission*: Annual audit reports, in the format prescribed by NITDA, shall be submitted to NITDA's designated submission portal within 30 days of audit completion. Reports shall include an executive summary, domain-by-domain compliance assessment, risk findings, and the FPI's remediation commitments.

(iii) *Internal Audit Interface*: Internal auditors shall present their audit programmes, audit plans, and findings to NITDA-accredited external auditors at the commencement of the annual external audit. NITDA-accredited auditors shall assess the adequacy of the internal audit function as part of their engagement scope.

(iv) *NITDA's Oversight Role*: NITDA shall analyse audit reports submitted by FPIs to identify sector-wide compliance patterns, systemic deficiencies, and emerging risk trends. NITDA shall publish an annual government-wide Information Security Compliance Report drawing on aggregate audit data. Individual FPI data shall be anonymised in the public version of this report unless an FPI is subject to an enforcement action.

(v) *Transitional Provision*: Pending the publication of the Cybersecurity Auditor Accreditation Framework, FPIs may engage auditors holding recognised international information security certifications (CISA, CISSP, ISO 27001 Lead Auditor, or equivalent) to discharge the first audit cycle under these Guidelines. NITDA shall publish the Accreditation Framework within six months of the Guidelines' effective date. FPIs shall be subjected to a mandatory annual third-party Information and Cyber Security audit, and this audit shall be conducted by NITDA accredited Information and Cyber Security Auditors. Annual audit reports shall be submitted to NITDA.

B3: NITDA-CERRT serves as the designated government-sector Computer Security Incident Response Team (CSIRT) for Federal Public Institutions. FPIs shall register with NITDA-CERRT and maintain current contact information in NITDA-CERRT's FPI directory.

NITDA-CERRT operates within the layered national CERT architecture established by the NCPS 2021, comprising: ngCERT

DRAFT

(national coordination, under NCCC) → Sectoral CSIRTs → Entity-level CERTs. Incidents reported to NITDA-CERRT that reach the threshold for national-level coordination shall be escalated to ngCERT in accordance with the NITDA-CERRT/ngCERT Coordination Protocol established by Memorandum of Understanding between NITDA and ONSA.

NITDA shall publish the incident classification thresholds, reporting templates, and escalation criteria applicable to NITDA-CERRT.

c) FPI's shall be required to have trained and certified personnel in the area of Information and Cyber Security or retain the services of an Information and Cyber Security expert.

d) Compliance Tiers. Obligations under these Guidelines are organised into three cumulative compliance tiers. Each FPI shall implement, at minimum, the tier corresponding to its risk classification as determined under the Statement of Applicability and confirmed at audit:

(a) Tier 1 — Minimum Baseline: mandatory for ALL FPIs without exception, irrespective of size, maturity, or risk exposure. Tier 1 constitutes the national security baseline.

(b) Tier 2 — Enhanced Controls: mandatory for medium-risk and digitally active FPIs (typically those at the Engaged or Optimised stage, or processing significant volumes of personal or sensitive data). Tier 2 includes all Tier 1 controls.

(c) Tier 3 — Advanced Controls: mandatory for high-impact FPIs, including those operating or supporting Critical National Information Infrastructure (CNII) and those at the Optimised or Transformed stage. Tier 3 includes all Tier 1 and Tier 2 controls.

An FPI's risk classification shall be reviewed at least annually and upon any material change to its systems, data holdings, or threat exposure.

e) FPIs should ensure full compliance with these guidelines within 12 months of release of this Guideline.

f) Compliance with these Guidelines shall be assessed solely against the requirements set out in these Guidelines. References to international standards and frameworks (including ISO/IEC 27001, ISO/IEC 27002, NIST, CIS Controls, COBIT, OWASP and PCI DSS) contained in Annex 1 are provided as implementation

DRAFT

and alignment guidance only and do not independently constitute compliance obligations for FPIs under these Guidelines.

12 Information Security Management Program Implementation Activities

a. Information Security Governance

Management shall lead and show leadership commitment to the information security program by:

a) establish an Information Security Steering Committee consisting of top management staff
b) ensuring that the resources needed for maintaining compliance to the information security management program as specified by this regulation are made available.
c) Communicating the significance of effective information security management and conformance to the requirements of this regulation;
d) guiding and encouraging employees to contribute to the information security management program's effectiveness.
e) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

b. Information Security Management Structure

Management shall ensure that roles relevant to the information security program are assigned and communicated with their respective responsibilities and authorities such roles include CISO, IS Managers, IS Internal Auditors, IS Implementers, IS Risk Managers and IS IS Compliance Team. To ensure that the information security program complies with the requirements of this regulation, top management shall:

a) Identify and designate a management representative responsible and accountable for information security management program.
b) Create an information security management team, which is in charge of implementing and managing the information security program as outlined in this regulation.
c) Information Security Manager is to evaluate and update top management on the performance of the information security management program.

DRAFT

The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:

a) Align with the statutory mandates of the organization;
b) Be consistent with the section 7 of this regulation;
c) Be measurable;
d) Take into account the requirements of this regulation, and results from risk assessment and risk treatment as provided in 12.5.2 and 12.5.3;
e) Be communicated;
f) Be updated as appropriate.

The organization shall define and document its information and cyber security objectives in a duly approved policy by its management and must answer the questions such as:

I. what will be done;
II. what resources will be required;
III. who will be responsible;
IV. when it will be completed;
V. how the results will be evaluated and
VI. corrective action measures

c. Support

The organization shall provide the necessary resources, competent personnel, and effective processes to implement and sustain the Information Security Management Program. This includes promoting awareness, ensuring clear communication, and maintaining properly controlled documented information.

i. Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the information security management program.

DRAFT

ii. Competence

The organization shall:

a) identify individuals with the necessary expertise to implement the information security program and, as needed, provide its staff with the necessary training to comply with the requirements of this regulation.

b) retain appropriate documented information as evidence of competence.

NOTE: Applicable actions may also include the hiring or contracting of competent persons.

iii. Awareness

All Personnel working for the organization are required to be aware of the following:

a) the organization's information security policy and its purpose;
b) the location of the organisation’s information security policy and other information security documents;
c) their contribution to the information security program's effectiveness, including the advantages of improved information security performance; and
d) the implications of not adhering to the program's requirements.
e) their knowledge of information Security policy and the overall information security management program should be tested at set intervals.

iv. Communication

The organization shall determine the need for internal and external communications relevant to the information security management program including:

a) on what to communicate;
b) when to communicate;
c) with whom to communicate;
d) who shall communicate;
e) the processes by which communication shall be effected.

v. Documented information

The organization’s information security management program shall include:

a) all documented information required by this regulation

DRAFT

b) documented information determined by the organization as being necessary for the effectiveness of the information security management program.

vi. Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g., a title, date, author, or reference number);
b) format (e.g., language, software version, graphics) and media (e.g., paper, electronic); and
c) review and approval for suitability and adequacy.

vii. Control of documented information

Documented information required by the information security management Program and by this regulation shall be controlled to ensure:

a) its availability and suitability; and
b) its protection (e.g., from loss of confidentiality, improper use, or loss of integrity).

The organization shall also address the following activities under control of documented information, as applicable:

i. distribution, access, retrieval and use;
ii. storage and preservation, including the preservation of legibility;
iii. control of changes (e.g., version control); and
iv. retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

DRAFT

d. Operations

i. The organization shall plan and control processes to meet information security requirements, including conducting risk assessments and implementing appropriate risk treatment measures. All activities shall be supported by documented information to ensure effective and consistent execution. Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in section 12.3 of this regulation. The organization shall also implement plans to achieve information and cyber security objectives determined in Section 7 of this regulation.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall ensure that outsourced processes are determined and controlled.

ii. Information security risk assessment

Organizations are required to establish an Information Security Risk Management methodology in line with global best practice such as the ISO/IEC 27005:2022 at planned intervals or when significant changes are proposed or occur and retain documented information of the results of the information security risk assessment.

iii. Information security risk treatment

The organization shall implement the information security risk treatment and retain documented information of the results as stipulated in the Guidelines on Information Security Risk Management for FPI's. The provisions stated in section 14.5 of this regulation should also be considered during risk treatment.

e. Performance evaluation

The organization shall evaluate the effectiveness of its Information Security Management Program through monitoring, measurement, internal audits, and periodic management reviews to ensure continuous improvement and alignment with objectives.

DRAFT

i. Monitoring, measurement, analysis and evaluation

The organization shall assess the effectiveness of its information security program. The organization shall determine:

a) what needs to be monitored and measured, including information and cyber security processes and controls;
b) The metrics (measure) for measurement;
c) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE The methods selected should produce comparable and reproducible results to be considered valid.

c) when the montoring and measuring shall be performed;
d) who shall monitor and measure;
e) when the results from monitoring and measurement shall be analysed and evaluated; and
f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

ii. Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management program:

a) conforms to
    1) the organization's requirements for its information security management program; and
    2) the requirements of this Guideline;
b) is effectively implemented and maintained.

The organization shall:

i. plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
ii. define the audit criteria and scope for each audit;
iii. Create an actionable audit plan and communicate the plan to all staff;
iv. ensure internal audits are conducted by the internal auditors as setup in 11(b) of this regulation;

DRAFT

v. ensure that the results of the audits are reported to relevant management; and
vi. retain documented information as evidence of the audit programme(s) and the audit results.
vii. Present audit programme, audit plan and audit report to NITDA accredited external Auditor during external audit.

iii. Management review

To ensure that the organization's information security management program remains appropriate, adequate, and effective, management shall review it at regular intervals. The management review shall take into account:

a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the information security management program;
c) feedback on the information and cyber security performance, including trends in:
1) nonconformities and corrective actions;
2) monitoring and measurement results;
3) audit results; and
4) fulfillment of information security objectives
d) feedback from interested parties;
e) results of risk assessment and status of risk treatment plan; and
f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management program. The organization shall retain documented information as evidence of the results of management reviews

f. Improvement

The organization shall address nonconformities through corrective actions, identify root causes, and prevent recurrence. It shall also continually improve the effectiveness, adequacy, and suitability of the Information Security Management Program while maintaining documented evidence.

DRAFT

i. Nonconformity and corrective action

When a non-conformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
   i. take action to control and correct it; and
   ii. deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   i. reviewing the nonconformity;
   ii. determining the causes of the nonconformity; and
   iii. determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management program, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:

   i. the nature of the nonconformities and any subsequent actions taken, and
   ii. the results of any corrective action

ii. Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management program.

13 Information Security Controls

A measure that addresses information or cyber risk is known as a control. While some of the controls in this document maintain risk, others modify it. For instance, a policy on information security can only maintain risk, whereas compliance with the policy can change risk. Additionally, some controls describe the same general measure in various risk contexts. This document offers a combination of organizational, People, physical, and technological information and cyber security controls drawn from extant statutory frameworks and international industry frameworks.

DRAFT

a. Determining controls

Controls are decided upon by the organization in response to a risk assessment with a clearly defined scope. Decisions regarding identified risks shall be based on the organization's risk management strategy, risk treatment options, and criteria for accepting risks. All applicable laws and regulations, both national and international shall be considered when determining the controls. The way controls interact with one another to provide defense in depth also plays a role in control determination.

Controls can be created by the organization as needed, or they can be found from any source. The organization should weigh the resources and investment required to implement and maintain a control against the business value realized when defining such controls.

The outcomes of a risk assessment shall serve as a guide for choosing the best course of action, setting priorities for handling information security risks, and putting in place the controls that were found to be required to mitigate these risks. Some of the controls in this document can be used by most organizations and are generally regarded as guiding principles for information security management.

14 Capability Maturity Model Integration (CMMI) Reference Model

The Federal Government of Nigeria recognizes the fact that Federal, State, Local Governments and their institutions are at different stages and phases of digital transformation and have varying priorities on their agenda towards building a digital economy. The level of Information security risk faced by organisation are usually proportional to the level of technology implementation.

Therefore, based on local and global realities, four (4) stages have been identified and defined to guide public institutions on their journey as they climb the digital transformation ladder. These stages will help public institutions to identify where they are along the digital transformation continuum. Additionally, organisations shall prepare a Statement of Applicability (SoA) to justify selected controls for implementation. IS Auditors shall refer to the SoA prior to commencement of audit.

DRAFT

a. Silo Stage

The main characteristics of a Silo stage include:

1. There is no or generally low adoption of ICT;
2. There is no recognition for a need of specific organizational IT/ICT policy;
3. Most of the organization data is on paper and few is captured in spreadsheet;
4. Applications and database are being introduced to enable certain services that are informational;
5. Digitized data does not follow any standard format;
6. The organization's existing IT infrastructure and applications only serve the need of the organization without consideration for a whole-of-government;
7. The organization has no proper structure established to be accountable for and to ensure compliance with agreed national and international IT/ICT related frameworks, guidelines, standards, best practices, models among others;
8. Less than 20% of the organization's processes are digitized; and
9. There is little or no capabilities to specify, deploy, manage and innovate with ICT systems, organizational processes and services.

b. Engaged Stage

The main characteristics of an engaged stage include:

1. There is moderate adoption of ICT;
2. There is awareness on having an organizational IT/ICT policy;
3. Most of the data is captured in spreadsheet and few on a database;
4. Applications and database are being introduced to make services interactive and dynamic;
5. There are standards already being considered for data digitization;
6. The organization's existing IT infrastructure and applications serve the need of the organization and few partners without full consideration for Ne-GIF, NGEA and other local and global Whole of Governemnt (WoG) requirements;
7. There is proposed governance structure established to be accountable for IT/ICT decision making and to ensure compliance with agreed national and international IT/ICT related frameworks, guidelines, standards, best practices, models among others;

DRAFT

8. Less than 30% of organization processes is digitized; and
9. There is element of capabilities to specify, deploy, manage and innovate with ICT systems, organizational processes and services.

c. Optimised Stage

Reaching the Optimised stage represents a significant milestone for an organization. Attainment of this stage positions public institutions to effectively support a WoG approach. The key characteristics of the Optimised stage include:

1. There is full adoption of ICT/digital technologies for organization's operations;
2. There exists an IT/ICT policy or strategy that ensures there is an organization's business and IT alignment;
3. There exists an IT Governance structure that is responsible and accountable for IT deployment decisions.
4. The existing IT Governance is also responsible for ensuring compliance with international and national IT/ICT related frameworks, guidelines, standards, best practices, models among others;
5. More than 80% of the organization's data is captured on database and databases are designed following global and national best practices and standards;
6. The deployment of ICT systems is in line with the provisions of the Nigeria Government Enterprise Architecture (NGEA), Nigeria e-Government Interoperability Framework (Ne-GIF) and other national and international regulations on IT/ICT design and management;
7. The organization's existing IT infrastructure and applications serve the need the organization and WoG requirements;
8. About 70% of organization's processes is digitized; and
9. There are capabilities to specify, deploy, manage and innovate with ICT projects, systems, organizational processes and services.

d. Transformed Stage

The transformed stage provides sufficient foundations for superior performance of the Government at all levels (Local, State and Federal). The way government operates fundamentally changed, and there is better

DRAFT

coherence, integration and coordination of processes, systems, services and businesses within and across government agencies, partners, and third parties at the Global, Federal, State and Local Governments respectively. The main characteristics of a digital transformation stage include:

1. There is full adoption of ICT/digital technologies based on all known global and national standards for organization's operations;
2. Digital technology and innovation is at the core of the organization's business transformation strategy;
3. The organization IT governance has been institutionalized, reached mature stage and is responsible for ensuring compliance with international and national IT/ICT related frameworks, guidelines, standards, best practices, models among others;
4. All the organization's data is captured on database, and databases are designed following global and national best practices and standards;
5. All organization's processes and data are digitized based on all known global and national standards;
6. The organization's existing IT infrastructure and applications serve the need the organization, WoG and digital transformation requirements;
7. There are capabilities across board (Federal, State and Local Governments) to specify, deploy, manage and innovate with ICT projects, systems, organizational processes and services;
8. Organization's IT/ICT systems and the enabling capabilities are highly compliant, responsive, stable, reliable, secure, scalable and cost-effective.
9. At the highest stage of digital transformation, the organization's IT infrastructure, applications and digital services are capable of providing citizens, businesses and customers, partners and third parties (within and outside Nigeria) with opportunities for online, financial and nonfinancial transactions end-to-end;
10. There is complete integration of IT systems by the Federal, State & Local Governments to provide digital services at local and global levels.

e. CMMI Information Security Controls Mapping

Digital Transformation brings forth unmatched opportunities and capabilities for growth and value creation. None of the opportunities, however, can be realized without dealing with the associated risks. Managing risks in the changing era is, thus, critical to an organization's sustainability. Table 2.0

DRAFT

serves as a prescriptive guide of minimum controls needed to tackle information security risk at the different stages of digital transformation. Organisations shall ascertain the stage which they currently are on their digital transformation journey as prescribed in this section, then consider applying the associated minimum controls as stated in Table 2.0 below as part of their risk treatment activities. Organisations shall prepare a Statement of Applicability (SoA) to justify selected controls for implementation. IS Auditors shall refer to the SoA prior to commencement of audit.

Table 2.0

Digital Transformation stage	**Risk Appetite**	**Minimum Controls**
Silo	Medium	All applicable controls in Domain 1, 2, 3, 4, 11, 12, 14
Engaged	Medium	All applicable controls in Domain 1, 2, 11, 12, 14,
Optimized	Low	Applicable Controls in all Domains
Transformed	Very Low	Applicable Controls in all Domains

Table 2.1 — Tier / Maturity Alignment [A1]

Tier	Typical CMMI Stage	Risk Profile	Control Set
Tier 1	Silo / Engaged	Baseline (all FPIs)	Foundational controls
Tier 2	Engaged / Optimised	Medium	Tier 1 + Enhanced
Tier 3	Optimised / Transformed	High / CNII	Tier 1 + 2 + Advanced

DRAFT

15 ANNEX 1

SCHEDULE OF INFORMATION SECURITY AND CYBER SECURITY CONTROLS FOR NIGERIAN GOVERNMENT FPIs

USAGE NOTE: *This schedule contains 78 controls across 15 domains. Each control includes a unique reference identifier, plain-language description, implementation guidance, and framework mapping to applicable international standards and Nigerian regulatory frameworks. The controls are to be directly referenced as compliance checklists and should be used during the implementation of information and cyber security programmes, especially during audits. Organisations should implement controls based on their risk profile and applicability.*

Organisations shall prepare a Statement of Applicability (SoA) to justify selected and excluded controls for implementation. IS Auditors shall refer to the SoA prior to commencement of audit.

Framework versions referenced: ISO/IEC 27001:2022, NIST CSF 2.0, CIS Controls v8, NIST SP 800-53 Rev 5, PCI DSS v4.0.1, OWASP Top 10 (2021), COBIT, NDPA 2023, Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 and National Cybersecurity Policy and Strategy (NCPS) 2021.

COMPLIANCE NOTE: Compliance is assessed against the requirements of these Guidelines only. The framework mapping column is provided as implementation and alignment guidance and does not create independent compliance obligations under any referenced standard (ISO 27001, NIST, CIS, COBIT, OWASP, PCI DSS, etc.).

FOUNDATIONAL ("P1") CONTROLS: The following controls are designated foundational "quick-win" controls and shall be implemented first by all FPIs, regardless of CMMI maturity stage: GRC-01, GRC-02, AM-01, AM-02, IAM-01, IAM-02, DP-01, DP-07, NET-01, VPM-01, MON-01, IR-01, IR-02, PHY-01, PPL-01 and TPR-01. A phased implementation schedule and sequencing logic for the remaining controls at each CMMI stage will be issued as a companion Implementation Prioritisation Guide.

.

DRAFT

DOMAIN 1: GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
GRC-01	Security Policy	The organisation shall establish, document, and maintain an information security policy approved by senior management, reviewed at least annually, and communicated to all personnel.	Policy should define security objectives, scope, roles, and management commitment.	ISO 27001 A.5.1; NIST CSF GV.PO; CIS v8 0
GRC-02	CISO Appointment	The organisation shall appoint a Chief Information Security Officer (CISO) or equivalent senior officer with direct reporting line to the head of the organisation.	CISO must be independent of IT operations to avoid conflicts of interest.	ISO 27001 A.5.2; NIST CSF GV.RR; COBIT APO13
GRC-03	Governance Committee	The organisation shall establish a cybersecurity governance committee (Steering Committee) at executive or board level that meets at least quarterly to review security posture, incidents, and risk.	Include legal, compliance, operations, and IT representation.	NIST CSF GV.OV; COBIT EDM03; ISO 27001 A.5.4
GRC-04	Risk Assessment	The organisation shall conduct a formal information security risk assessment at least annually and whenever significant changes occur to systems, processes, or the threat environment.	Use ISO 27005, NIST SP 800-30, FAIR, or OCTAVE methodology.	ISO 27001 6.1.2; NIST CSF ID.RA; NIST 800-53 RA

DOMAIN 1: GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
GRC-05	Risk Register	The organisation shall maintain a risk register documenting identified risks, risk owners, treatment decisions, residual risk levels, and review dates.	Review and update quarterly.	ISO 27001 6.1.3; NIST CSF ID.RA; COBIT APO12
GRC-06	Regulatory Compliance	The organisation shall identify all applicable legal, regulatory, and contractual information security requirements and maintain evidence of compliance.	Include sector-specific regulations.	ISO 27001 A.5.31–5.36; NIST CSF GV.OC; COBIT MEA03
GRC-07	Roles & Responsibilities	The organisation shall define and assign information security roles and responsibilities for all personnel, including asset owners, administrators, and data custodians.	Document in job descriptions and terms of employment.	ISO 27001 A.5.2–5.4; NIST CSF GV.RR; NIST 800-53 PS

DOMAIN 2: ASSET MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
AM-01	Hardware Inventory	The organisation shall maintain a complete and accurate inventory of all hardware assets connected to the network, updated within 24 hours of any change.	Use automated discovery and inventory tools.	CIS v8 1; ISO 27001 A.5.9; NIST CSF ID.AM; NIST 800-53 CM-8

DOMAIN 2: ASSET MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
AM-02	Software Inventory	The organisation shall maintain a complete inventory of all authorised software, including versions and patch levels, and prevent installation of unauthorised software.	Use application whitelisting and software management tools.	CIS v8 2; ISO 27001 A.5.9; NIST CSF ID.AM; NIST 800-53 CM-8
AM-03	Data Classification	The organisation shall classify all information assets by criticality and sensitivity (Public, Internal, Confidential, Restricted) and apply handling requirements proportionate to classification.	Conduct risk assessment on all organization information to determine their level of criticality and sensitivity.	CIS v8 3; ISO 27001 A.5.10–5.13; NIST 800-53 RA-2
AM-04	Asset Ownership	The organisation shall assign an owner for every information asset, responsible for access controls, classification, and protection throughout its lifecycle.	Review asset ownership annually.	ISO 27001 A.5.9; NIST CSF ID.AM
AM-05	Secure Disposal	The organisation shall establish procedures for secure disposal or re-use of equipment and storage media using cryptographic erasure, degaussing, or physical destruction.	Maintain disposal records and certificates of destruction.	ISO 27001 A.7.10, A.7.14; NIST 800-53 MP-6; PCI DSS 9.4

DOMAIN 3: IDENTITY AND ACCESS MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
IAM-01	Access Control	The organisation shall implement role-based access control (RBAC) granting access based on least privilege and need-to-know. All access rights shall be recertified at least quarterly.	Document access approval and recertification processes.	CIS v8 6; ISO 27001 A.5.15–5.18; NIST 800-53 AC-2; PCI DSS 7
IAM-02	Multi-Factor Auth	The organisation shall enforce multi-factor authentication (MFA) for all users, with phishing-resistant MFA (FIDO2/WebAuthn) mandatory for privileged accounts.	Eliminate SMS-based OTP; it is vulnerable to SIM swap attacks.	CIS v8 6; ISO 27001 A.8.5; NIST 800-53 IA-2; PCI DSS 8.4
IAM-03	Password Policy	The organisation shall enforce passwords of minimum 8 characters with a combination of alphanumeric and special characters. Blocklist commonly breached passwords and prohibition of reuse across the last 24 passwords. Enforce password change every 90 days.	Leverage password complexity features inherent in applications.	NIST SP 800-63B; ISO 27001 A.8.5; CIS v8 5; PCI DSS 8.3
IAM-04	Privileged Access	The organisation shall manage privileged accounts through a PAM solution with just-in-time (JIT) access, session recording, and	No standing administrative privileges; all elevated access must be time-bounded.	CIS v8 6; ISO 27001 A.8.2; NIST 800-53 AC-6; PCI DSS 8.6

DOMAIN 3: IDENTITY AND ACCESS MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		automatic credential rotation.		
IAM-05	Service Accounts	The organisation shall inventory all service accounts, eliminate shared and default passwords, and store secrets in a dedicated secrets management platform.	No hardcoded credentials in source code, scripts, or config files.	CIS v8 5; ISO 27001 A.8.4; NIST 800-53 IA-5
IAM-06	Account Lifecycle	The organisation shall disable accounts within 24 hours of staff termination or role change and conduct quarterly reviews to remove orphaned or dormant accounts.	Integrate HR systems with identity management for automated provisioning.	CIS v8 5; ISO 27001 A.5.18, A.6.5; NIST 800-53 AC-2; PCI DSS 8.1
IAM-07	Remote Access	The organisation shall secure remote access through Zero Trust Network Access (ZTNA) or Virtual Private Network (VPN) with Multi Factor Authentication (MFA) and device posture verification. Direct RDP, SSH, or database access from the internet is prohibited.	Replace legacy VPN with ZTNA where feasible.	CIS v8 12; ISO 27001 A.8.1; NIST 800-53 AC-17

DOMAIN 4: DATA PROTECTION AND PRIVACY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
DP-01	Encryption at Rest	The organisation shall encrypt all sensitive data at rest using AES-256 or equivalent, with keys managed through a dedicated KMS or HSM, separate from encrypted data.	Implement Transparent Data Encryption (TDE) on all databases.	ISO 27001 A.8.24; NIST 800-53 SC-28; PCI DSS 3.5; CIS v8 3
DP-02	Encryption in Transit	The organisation shall encrypt all data in transit using TLS 1.3 (minimum TLS 1.2) externally and mTLS for internal service-to-service communications. Unencrypted protocols shall be disabled.	Enforce HSTS; disable TLS 1.0 and 1.1.	ISO 27001 A.8.24; NIST 800-53 SC-8; PCI DSS 4.2; CIS v8 3
DP-03	Data Loss Prevention	The organisation shall deploy DLP controls at network, endpoint, and cloud layers to detect and prevent unauthorised transmission of classified or personal data.	Tune DLP to reduce false positives while covering sensitive data patterns (NIN, BVN, passport).	CIS v8 3; ISO 27001 A.8.12; NIST 800-53 SI-4; PCI DSS 3
DP-04	Data Masking	The organisation shall apply data masking or pseudonymisation to personal data in non-production environments. Real personal data shall never be used outside production.	Use irreversible masking or synthetic data generation.	ISO 27001 A.8.11; NIST 800-53 PT-5; NDPA 2023 s.29

DOMAIN 4: DATA PROTECTION AND PRIVACY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
DP-05	Data Retention	The organisation shall enforce a data retention policy with maximum retention periods per data category and automated deletion or anonymisation upon expiry.	Align with NDPA 2023 purpose and storage limitation principles.	ISO 27001 A.5.33; NIST 800-53 SI-12; NDPA 2023 s.25
DP-06	Backup & Recovery	The organisation shall maintain encrypted backups following the 3-2-1-1 rule (3 copies, 2 media, 1 offsite, 1 immutable). Test restoration monthly; conduct DR exercises quarterly.	Immutable backups prevent ransomware from encrypting backup copies.	CIS v8 11; ISO 27001 A.8.13; NIST 800-53 CP-9; PCI DSS 9
DP-07	Breach Notification	The organisation shall notify the NDPC within 72 hours of becoming aware of a breach, and notify affected data subjects without undue delay where the breach poses high risk to their rights.	Maintain pre-drafted notification templates and assessment checklists.	NDPA 2023 s.39–40; ISO 27001 A.5.24; NIST CSF RS.CO

DOMAIN 5: NETWORK AND INFRASTRUCTURE SECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
NET-01	Segmentation	The organisation shall segment its network into security zones (DMZ, internal, database, management, guest) with	Document business justification for every inter-zone rule.	CIS v8 12; ISO 27001 A.8.22; NIST 800-53 SC-7; PCI DSS 1

DOMAIN 5: NETWORK AND INFRASTRUCTURE SECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		explicit allow-list firewall rules. Database servers shall have no direct internet connectivity.		
NET-02	Firewall Management	The organisation shall deploy NGFWs at all perimeters and zone boundaries, with rules reviewed quarterly to remove stale or overly permissive entries.	Document business justification for every firewall rule.	CIS v8 12; ISO 27001 A.8.20–8.22; NIST 800-53 SC-7; PCI DSS 1
NET-03	Egress Filtering	The organisation shall control all outbound traffic through an inspecting proxy. Direct outbound internet from servers, databases, and internal applications shall be blocked.	Egress allow-listing prevents data exfiltration to attacker infrastructure.	CIS v8 13; NIST 800-53 SC-7; PCI DSS 1; MITRE ATT&CK T1041
NET-04	DNS Security	The organisation shall implement DNS filtering and monitoring to block access to known malicious domains and C2 infrastructure.	Use DNS sinkholing and threat intelligence feeds.	CIS v8 9; NIST 800-53 SC-20; ISO 27001 A.8.23
NET-05	Wireless Security	The organisation shall secure wireless networks using WPA3 Enterprise with 802.1X, separate guest from internal networks, and scan quarterly for rogue access points.	Maintain an inventory of all authorised wireless access points.	CIS v8 12; ISO 27001 A.8.20; NIST 800-53 AC-18

DOMAIN 5: NETWORK AND INFRASTRUCTURE SECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
NET-06	Intrusion Detection	The organisation shall deploy NDR or IDS/IPS at boundaries and between critical zones, with daily signature updates and anomaly detection enabled.	ML-based NDR detects distributed, low-volume exfiltration patterns.	CIS v8 13; ISO 27001 A.8.16; NIST 800-53 SI-4; PCI DSS 11.4

DOMAIN 6: SECURE CONFIGURATION AND CHANGE MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
SCM-01	Secure Baselines	The organisation shall enforce hardened configuration baselines for all systems based on CIS Benchmarks or equivalent, with automated compliance monitoring.	Automate checks using configuration management tools.	CIS v8 4; ISO 27001 A.8.9; NIST 800-53 CM-2; PCI DSS 2
SCM-02	Change Management	The organisation shall implement formal change management including risk assessment, approval, testing, rollback procedures, and post-change verification for all production changes.	Emergency changes must be retrospectively documented within 48 hours.	ISO 27001 A.8.32; NIST 800-53 CM-3; PCI DSS 6.5; ITIL 4
SCM-03	Environment Separation	The organisation shall maintain strict separation between development, testing, and production environments. Production data shall not be used in	Non-production environments must not connect to production networks.	ISO 27001 A.8.31; NIST 800-53 CM-4; PCI DSS 6.5

DOMAIN 6: SECURE CONFIGURATION AND CHANGE MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		non-production without masking.		
SCM-04	Default Credentials	The organisation shall change all vendor defaults, remove unnecessary accounts and services, and verify before production deployment.	Automate default credential detection during provisioning.	CIS v8 4; ISO 27001 A.8.9; PCI DSS 2.1; NIST 800-53 CM-6

DOMAIN 7: VULNERABILITY AND PATCH MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
VPM-01	Vulnerability Scanning	The organisation shall scan all external assets weekly and internal assets fortnightly. Non-production and pilot environments shall be included in scope.	Use enterprise vulnerability scanners with authenticated scanning.	CIS v8 7; ISO 27001 A.8.8; NIST 800-53 RA-5; PCI DSS 11.3
VPM-02	Patch SLAs	The organisation shall patch Critical (CVSS 9.0+) within 48 hours, High (7.0–8.9) within 7 days, Medium (4.0–6.9) within 30 days, Low (<4.0) within 90 days. KEV vulnerabilities within 48 hours regardless of CVSS.	Track patching compliance as a KPI reported to management monthly.	CIS v8 7; ISO 27001 A.8.8; NIST 800-53 SI-2; PCI DSS 6.3
VPM-03	Attack Surface Management	The organisation shall continuously discover and monitor all internet-exposed assets using an	Include subdomains, APIs, cloud	CIS v8 1; NIST CSF ID.AM; NIST 800-53 CM-8

DOMAIN 7: VULNERABILITY AND PATCH MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		EASM platform. Unapproved exposed assets shall be immediately isolated.	resources, and shadow IT.	
VPM-04	Penetration Testing	The organisation shall conduct external penetration testing annually (and after major changes) and internal testing annually, by an independent accredited provider. Critical findings shall be retested within 30 days.	Include web applications, APIs, VPN, and cloud infrastructure.	CIS v8 18; ISO 27001 A.8.8; NIST 800-53 CA-8; PCI DSS 11.3

DOMAIN 8: APPLICATION AND API SECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
APP-01	Secure SDLC	The organisation shall integrate security into the SDLC: secure coding standards, threat modelling, peer code review, and SAST/DAST before production deployment.	Adopt OWASP Top 10 and OWASP ASVS as baselines.	CIS v8 16; ISO 27001 A.8.25–8.31; NIST 800-53 SA-11; PCI DSS 6
APP-02	WAF	The organisation shall deploy a WAF in blocking mode on all internet-facing web applications, protecting against OWASP Top 10 vulnerabilities.	Update WAF rules promptly for newly disclosed vulnerabilities.	CIS v8 13; ISO 27001 A.8.23; NIST 800-53 SC-7; PCI DSS 6.4

DOMAIN 8: APPLICATION AND API SECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
APP-03	API Security	The organisation shall secure APIs with OAuth 2.0/OIDC, rate limiting, input validation, and centralised API gateway. No unauthenticated API endpoints shall exist.	Implement mTLS for backend API communications.	ISO 27001 A.8.28; NIST 800-53 SC-7; OWASP API Top 10
APP-04	Security Headers	The organisation shall implement CSP, HSTS, X-Content-Type-Options, X-Frame-Options, and Referrer-Policy on all web applications.	Include security header validation in CI/CD pipeline.	OWASP; ISO 27001 A.8.28; NIST 800-53 SC-8

DOMAIN 9: SECURITY MONITORING AND LOGGING				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
MON-01	Centralised Logging	The organisation shall aggregate audit logs from all systems in a centralised SIEM. Logs shall be retained 12 months online and 24 months archived, with tamper-proof storage.	Cover firewalls, servers, databases, endpoints, auth systems, and cloud.	CIS v8 8; ISO 27001 A.8.15; NIST 800-53 AU-6; PCI DSS 10
MON-02	SOC	The organisation shall establish or engage a 24/7 SOC with documented playbooks. MTTD target: <1 hour for critical alerts; MTTR target: <4 hours.	Engage MDR provider if in-house SOC is not feasible.	ISO 27001 A.5.24; NIST CSF DE.CM; CIS v8 13
MON-03	EDR	The organisation shall deploy EDR in active	Ensure coverage across all OS	CIS v8 10; ISO 27001 A.8.7; NIST

DOMAIN 9: SECURITY MONITORING AND LOGGING				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		response mode on all endpoints and servers (including Linux), with automatic isolation of compromised systems.	types, not only Windows.	800-53 SI-3; MITRE ATT&CK
MON-04	NDR	The organisation shall deploy NDR to baseline traffic and alert on anomalies including unusual data volumes, known-bad IPs, and lateral movement indicators.	ML-based anomaly detection is critical for advanced exfiltration.	CIS v8 13; ISO 27001 A.8.16; NIST 800-53 SI-4
MON-05	Database Monitoring	The organisation shall implement DAM on all sensitive databases, alerting on bulk queries, export operations, and unusual source addresses. Threshold: >10,000 records triggers alert.	DAM should trigger automatic temporary account lockout.	ISO 27001 A.8.15; NIST 800-53 AU-12; PCI DSS 10
MON-06	UEBA	The organisation shall implement UEBA to detect anomalous login patterns, geographic impossibility, privilege escalation, and mass file access, integrated with SIEM.	Use automated risk scoring for user accounts.	NIST 800-53 AC-2(12); ISO 27001 A.8.16; MITRE ATT&CK

DOMAIN 10: INCIDENT RESPONSE AND BUSINESS CONTINUITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
IR-01	IR Plan	The organisation shall maintain an IRP defining roles, communications, escalation, and pre-authorised containment actions, aligned with NIST SP 800-61r2.	SOC analysts must have pre-authorised containment authority.	CIS v8 17; ISO 27001 A.5.24–5.28; NIST 800-53 IR-1; PCI DSS 12.10
IR-02	Incident Reporting	The organisation shall report cyber incidents to NITDA-CERRT within 72 hours (Cybercrimes Act 2024) and data breaches to NDPC within 72 hours (NDPA 2023).	Maintain pre-drafted reporting templates.	Cybercrimes Act 2024 s.21; NDPA 2023 s.39; NIST 800-53 IR-6
IR-03	Exercises	The organisation shall conduct tabletop exercises quarterly and full-scale simulations annually covering ransomware, exfiltration, insider threat, and supply chain scenarios.	Include executive leadership in exercises.	CIS v8 17; ISO 27001 A.5.24; NIST 800-53 IR-3; PCI DSS 12.10
IR-04	Digital Forensics	The organisation shall maintain or retain access to digital forensics capability for evidence preservation, collection, analysis, and reporting with chain-of-custody compliance.	Establish retainer agreements with forensics providers.	ISO 27001 A.5.28; NIST 800-53 IR-4; NIST SP 800-86
IR-05	Business Continuity	The organisation shall maintain BCP/DR plans tested annually through simulation, with documented RTOs and	Include cyber incident scenarios in BCP testing.	ISO 27001 A.5.29–5.30; NIST 800-53 CP; CIS v8 11; PCI DSS 12

DOMAIN 10: INCIDENT RESPONSE AND BUSINESS CONTINUITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		RPOs. Critical systems: RTO 4 hours, RPO 1 hour.		

DOMAIN 11: PHYSICAL AND ENVIRONMENTAL SECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
PHY-01	Physical Access	The organisation shall restrict data centre, server room and other secure area access to authorised personnel using physical controls (manual lock, card, biometric). Maintain visitor logs.	Escort all visitors in secure areas.	ISO 27001 A.7.1–7.6; NIST 800-53 PE; PCI DSS 9
PHY-02	Environmental	The organisation shall protect critical infrastructure against fire, flood, power failure, and temperature extremes with fire suppression, monitoring, and redundant power.	Implement automated environmental alerts.	ISO 27001 A.7.5, A.7.8–7.12; NIST 800-53 PE-10–15
PHY-03	Clear Desk/Screen	The organisation shall enforce clear desk and clear screen policies. Automated screen lock shall activate after 3 minutes of inactivity.	Include in security awareness training.	ISO 27001 A.7.7; NIST 800-53 AC-11

DOMAIN 12: PEOPLE AND AWARENESS				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
PPL-01	Security Training	The organisation shall deliver mandatory cybersecurity awareness training on onboarding and at least annually, covering phishing, social engineering, password hygiene, data handling, and incident reporting.	Track completion rates; enforce consequences for non-compliance.	CIS v8 14; ISO 27001 A.6.3; NIST 800-53 AT; PCI DSS 12.6
PPL-02	Phishing Simulation	The organisation shall conduct phishing simulations at least monthly. Staff who repeatedly fail shall undergo immediate additional training.	Simulate current TTPs including spear-phishing and BEC.	CIS v8 14; NIST 800-53 AT-2; ISO 27001 A.6.3
PPL-03	Personnel Screening	The organisation shall conduct background checks on all personnel before employment, proportionate to the sensitivity of the role and data access.	Enhanced screening for privileged and sensitive data access roles.	ISO 27001 A.6.1; NIST 800-53 PS-3
PPL-04	Privileged User Training	The organisation shall provide annual advanced security training to privileged users covering secure administration, credential management, insider threat, and IR procedures.	Include hands-on practical exercises.	CIS v8 14; ISO 27001 A.6.3; NIST 800-53 AT-3

DOMAIN 13: SUPPLY CHAIN AND THIRD-PARTY RISK MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
TPR-01	Supplier Assessment	The organisation shall assess cybersecurity posture of all third parties with system or data access before engagement and annually thereafter.	Maintain risk-rated supplier register.	CIS v8 15; ISO 27001 A.5.19–5.23; NIST 800-53 SR; NIST CSF GV.SC
TPR-02	Contractual Security	The organisation shall include security requirements in all third-party contracts: data protection, breach notification within 24 hours, right-to-audit, and defined data handling and destruction.	Specify permitted processing locations and sub-processor restrictions.	ISO 27001 A.5.20; NIST 800-53 SA-4; NDPA 2023 s.30
TPR-03	Third-Party Access	The organisation shall provide third-party access through isolated network segments with dedicated credentials, time-limited sessions, and full logging. No direct core database access.	Route through hardened DMZ with API gateway.	CIS v8 15; ISO 27001 A.5.19; NIST 800-53 AC-20; PCI DSS 12.8
TPR-04	Cloud Security	The organisation shall ensure cloud providers meet security requirements with contractual data sovereignty, encryption, access controls, incident notification, and right-to-audit provisions. In addition, the organisation shall: (i) adopt a cloud security	Align with CSA CCM v4.0.	ISO 27001 A.5.23; NIST 800-53 SA-9; CSA CCM v4.0

DOMAIN 13: SUPPLY CHAIN AND THIRD-PARTY RISK MANAGEMENT				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		governance framework appropriate to government use; (ii) document and apply the shared responsibility model, clearly delineating the security obligations of the FPI and of the cloud service provider; (iii) require cloud assurance and certification evidence from providers (e.g. ISO/IEC 27017, ISO/IEC 27018 or equivalent independent attestation); (iv) extend these requirements to third-party hosting, co-location and hybrid hosting arrangements; and (v) align cloud adoption with government cloud and data-sovereignty initiatives, including applicable Galaxy Backbone policies.		

DOMAIN 14: AI-DRIVEN CYBERSECURITY THREATS				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
AI-01	AI Threat Awareness	The organisation shall incorporate AI-driven attack techniques into its risk assessment	Update threat intelligence and risk registers to	NIST AI RMF 1.0; NIST CSF ID.RA; ISO 27001 A.5.7; MITRE ATLAS

DOMAIN 14: AI-DRIVEN CYBERSECURITY THREATS				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		programme, including AI-generated phishing, deepfake social engineering, automated vulnerability exploitation, and adversarial machine learning attacks.	account for AI-enhanced TTPs.	
AI-02	Deepfake Detection	The organisation shall implement controls to detect and mitigate deepfake-based social engineering attacks, including AI-generated voice, video, and image manipulation used for impersonation of executives, clients, or authority figures.	Establish out-of-band verification procedures for high-value authorisations (wire transfers, credential resets, access grants) that cannot rely on voice or video alone.	NIST AI RMF 1.0 MAP-2; MITRE ATLAS; ISO 27001 A.5.14
AI-03	AI-Enhanced Phishing Defence	The organisation shall deploy AI-powered email security solutions capable of detecting and blocking AI-generated phishing emails, which may bypass traditional signature and keyword-based filters due to their linguistic sophistication.	Use NLP-based analysis, sender behaviour profiling, and anomaly detection rather than relying solely on content-based filtering.	CIS v8 9; ISO 27001 A.8.23; NIST 800-53 SI-8; NIST AI RMF 1.0
AI-04	Automated Attack Detection	The organisation shall deploy security monitoring tools capable of detecting AI-automated attack patterns, including rapid, adaptive scanning and	Implement behavioural analysis and ML-based detection that adapts to novel attack	NIST 800-53 SI-4; ISO 27001 A.8.16; CIS v8 13; MITRE ATLAS

DOMAIN 14: AI-DRIVEN CYBERSECURITY THREATS				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		exploitation sequences, automated credential stuffing at scale, and polymorphic malware generated by AI.	patterns rather than relying on static signatures.	
AI-05	AI System Security	The organisation shall secure any AI or machine learning systems it deploys (including chatbots, decision-support tools, and automated processes) against adversarial attacks, including data poisoning, model manipulation, prompt injection, and training data extraction.	Apply OWASP Top 10 for LLM Applications where applicable. Implement input validation, output filtering, and access controls on AI models.	NIST AI RMF 1.0; OWASP LLM Top 10; MITRE ATLAS; ISO 42001
AI-06	AI Governance	The organisation shall establish a governance framework for the use of AI technologies that addresses data privacy, security risks, ethical considerations, and regulatory compliance. AI tools shall not process classified or sensitive data without prior risk assessment and approval.	Maintain a register of all AI tools in use, including shadow AI adopted without IT approval.	ISO/IEC 42001; NIST AI RMF 1.0; EU AI Act (reference); NDPA 2023
AI-07	GenAI Data Leakage	The organisation shall implement controls to prevent the leakage of sensitive, classified, or personal data through	Block or restrict access to public GenAI services from corporate networks.	NIST AI RMF 1.0; ISO 27001 A.8.12; CIS v8 3; NDPA 2023 s.24

DOMAIN 14: AI-DRIVEN CYBERSECURITY THREATS				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		Generative AI tools (ChatGPT, Copilot, etc.), including DLP policies that monitor and block sensitive data in AI prompts and inputs.	Approved GenAI tools must be sandboxed with no access to production data.	
AI-08	AI-Augmented SOC	The organisation shall evaluate and adopt AI-powered security operations capabilities, including AI-assisted threat detection, automated alert triage, and AI-driven incident response playbook execution, to address the speed and scale of AI-enabled attacks.	AI augmentation should supplement, not replace, human analyst judgement in the SOC.	NIST CSF DE.AE; ISO 27001 A.8.16; NIST 800-53 SI-4

DOMAIN 15: POST-QUANTUM CYBERSECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
PQC-01	Cryptographic Inventory	The organisation shall create and maintain a comprehensive inventory of all cryptographic assets, including algorithms, key sizes, protocols, certificates, libraries, and hardware modules in use across the organisation.	Identify all instances of RSA, ECC, Diffie-Hellman, and other public-key algorithms that are vulnerable to quantum attack.	NIST SP 1800-38B; ISO 27001 A.8.24; NIST CSF PR.DS; CNSA 2.0

DOMAIN 15: POST-QUANTUM CYBERSECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
PQC-02	Quantum Risk Assessment	The organisation shall conduct a quantum risk assessment to identify systems, data, and communications most vulnerable to quantum-enabled attacks, considering data sensitivity, classification, regulatory requirements, and the expected shelf life of encrypted data.	Prioritise data with long confidentiality requirements (state secrets, health records, identity data) that could be harvested now and decrypted when quantum computing becomes viable ("harvest now, decrypt later" threat).	NIST IR 8547; NIST SP 1800-38B; ISO 27001 6.1.2; ETSI QSC
PQC-03	PQC Migration Plan	The organisation shall develop a post-quantum cryptography migration plan with defined timelines for transitioning to quantum-resistant algorithms such as ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205).	Plan should include hybrid approaches (combining classical and PQC algorithms) during the transition period to maintain backward compatibility.	NIST FIPS 203, 204, 205; NIST SP 1800-38; CNSA 2.0; ETSI QSC
PQC-04	Crypto Agility	The organisation shall design and implement cryptographic systems with crypto-agility, enabling the rapid replacement of cryptographic algorithms,	Use abstraction layers and configuration-driven cryptographic selections rather	NIST SP 1800-38B; ISO 27001 A.8.24; NIST IR 8547

DOMAIN 15: POST-QUANTUM CYBERSECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		key sizes, and protocols without requiring fundamental architectural changes to applications or infrastructure.	than hardcoded algorithms.	
PQC-05	TLS/PKI Readiness	The organisation shall assess and prepare its TLS infrastructure, PKI, and certificate management systems for compatibility with post-quantum algorithms, including support for hybrid TLS certificates and quantum-resistant key exchange mechanisms.	Monitor browser, server, and CA vendor readiness for PQC certificate support. Test hybrid TLS in non-production environments.	NIST SP 1800-38; IETF RFC 9180; CNSA 2.0; ISO 27001 A.8.24
PQC-06	VPN & Comms Security	The organisation shall evaluate and plan for post-quantum VPN and secure communications solutions, ensuring that IPsec, WireGuard, and other tunnel protocols can support quantum-resistant key exchange (e.g., ML-KEM-based IKEv2).	Prioritise VPN migration for systems carrying classified or highly sensitive government data.	NIST SP 1800-38; CNSA 2.0; ISO 27001 A.8.20; NIST 800-53 SC-8
PQC-07	Digital Signatures	The organisation shall plan for the migration of digital signature schemes to quantum-resistant algorithms (ML-DSA/FIPS 204 or SLH-DSA/FIPS	Start with non-critical systems and expand to production after validation.	NIST FIPS 204, 205; CNSA 2.0; ISO 27001 A.8.24

DOMAIN 15: POST-QUANTUM CYBERSECURITY				
Ref.	**Control Domain**	**Control Requirement**	**Implementation Guidance**	**Framework Reference**
		205) for code signing, document signing, authentication tokens, and certificate issuance.		
PQC-08	Quantum Key Distribution	The organisation shall monitor developments in Quantum Key Distribution (QKD) technology and assess its applicability for protecting the highest-sensitivity communications and data, while recognising current limitations in distance, infrastructure cost, and standardisation maturity.	QKD is not a near-term replacement for PQC algorithms but may complement them for ultra-high-assurance channels.	ETSI QKD; ISO 27001 A.8.24; ITU-T Y.3800 series

DRAFT

16 ANNEX 2

ACRONYMS AND ABBREVIATIONS

Acronym	Full Meaning	Category
8		
802.1X	IEEE Standard for Port-Based Network Access Control	*Network Security*
A		
AES	Advanced Encryption Standard	*Cryptography*
AI	Artificial Intelligence	*AI Security*
API	Application Programming Interface	*Application Security*
ASVS	Application Security Verification Standard	*Application Security*
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	*Threat Intelligence*
ATLAS	Adversarial Threat Landscape for AI Systems	*AI Security*
B		
BCP	Business Continuity Plan	*Business Continuity*
BEC	Business Email Compromise	*Threat Type*
BVN	Bank Verification Number	*Nigerian Context*
C		
C2	Command and Control	*Threat Intelligence*
CA	Certificate Authority	*Cryptography*
CCM	Cloud Controls Matrix	*Cloud Security*
CERT	Computer Emergency Response Team	*Incident Response*
CI/CD	Continuous Integration / Continuous Deployment	*Software Development*
CIS	Center for Internet Security	*Framework / Standard*
CISO	Chief Information Security Officer	*Governance*

Acronym	Full Meaning	Category
CMMI	Capability Maturity Model Integration	*Framework / Standard*
CNSA	Commercial National Security Algorithm (NSA Suite)	*Cryptography*
COBIT	Control Objectives for Information and Related Technologies	*Framework / Standard*
CSA	Cloud Security Alliance	*Cloud Security*
CSF	Cybersecurity Framework	*Framework / Standard*
CSP	Content Security Policy	*Application Security*
CVSS	Common Vulnerability Scoring System	*Vulnerability Management*
D		
DAM	Database Activity Monitoring	*Security Monitoring*
DAST	Dynamic Application Security Testing	*Application Security*
DLP	Data Loss Prevention	*Data Protection*
DMZ	Demilitarised Zone	*Network Security*
DNS	Domain Name System	*Network Security*
DPO	Data Protection Officer	*Governance / Privacy*
DR	Disaster Recovery	*Business Continuity*
E		
EASM	External Attack Surface Management	*Vulnerability Management*
ECC	Elliptic Curve Cryptography	*Cryptography*
EDR	Endpoint Detection and Response	*Security Monitoring*
ETSI	European Telecommunications Standards Institute	*Standards Body*
EU	European Union	*Regulatory*
F		
FAIR	Factor Analysis of Information Risk	*Risk Management*

Acronym	Full Meaning	Category
FIDO2	Fast Identity Online (version 2)	*Identity & Access*
FIPS	Federal Information Processing Standards	*Framework / Standard*
FPI	Federal Public Institutions	*Nigerian Context*
G		
GAID	General Application and Implementation Directive	*Nigerian Context*
GenAI	Generative Artificial Intelligence	*AI Security*
GRC	Governance, Risk and Compliance	*Governance*
H		
HR *	Human Resources	*Governance*
HSM	Hardware Security Module	*Cryptography*
HSTS	HTTP Strict Transport Security	*Application Security*
I		
IAM	Identity and Access Management	*Identity & Access*
ICT	Information and Communications Technology	*Infrastructure*
IDS	Intrusion Detection System	*Network Security*
IEC	International Electrotechnical Commission	*Standards Body*
IETF	Internet Engineering Task Force	*Standards Body*
IKEv2	Internet Key Exchange version 2	*Network Security*
IoT	Internet of Things	*Infrastructure*
IPS	Intrusion Prevention System	*Network Security*
IPsec	Internet Protocol Security	*Network Security*
IR	Incident Response	*Incident Response*
IRP	Incident Response Plan	*Incident Response*
IS	Information Security	*Governance*
ISMS	Information Security Management System	*Governance*

Acronym	Full Meaning	Category
ISO	International Organization for Standardization	*Standards Body*
IT	Information Technology	*Infrastructure*
ITIL	Information Technology Infrastructure Library	*Framework / Standard*
ITU-T	International Telecommunication Union – Telecommunication Standardisation Sector	*Standards Body*
J		
JIT	Just-In-Time (access provisioning)	*Identity & Access*
K		
KEV	Known Exploited Vulnerabilities (CISA catalogue)	*Vulnerability Management*
KMS	Key Management Service	*Cryptography*
KPI	Key Performance Indicator	*Governance*
L		
LLM	Large Language Model	*AI Security*
M		
MDR	Managed Detection and Response	*Security Monitoring*
MFA	Multi-Factor Authentication	*Identity & Access*
MITRE	Massachusetts Institute of Technology Research Establishment (now a proper name)	*Threat Intelligence*
ML	Machine Learning	*AI Security*
ML-DSA	Module-Lattice-Based Digital Signature Algorithm (FIPS 204)	*Post-Quantum Cryptography*
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism (FIPS 203)	*Post-Quantum Cryptography*
MTTD	Mean Time to Detect	*Security Monitoring*
MTTR	Mean Time to Respond	*Incident Response*
mTLS	Mutual Transport Layer Security	*Cryptography*

Acronym	Full Meaning	Category
N		
NCPS	National Cybersecurity Policy and Strategy	*Nigerian Context*
NDR	Network Detection and Response	*Security Monitoring*
NDPA	Nigeria Data Protection Act	*Nigerian Context*
NDPC	Nigeria Data Protection Commission	*Nigerian Context*
Ne-GIF	Nigeria e-Government Interoperability Framework	*Nigerian Context*
NGEA	Nigeria Government Enterprise Architecture	*Nigerian Context*
NGFW	Next-Generation Firewall	*Network Security*
ngCERT	National Computer Emergency Response Team (Nigeria)	*Nigerian Context*
NIN	National Identification Number	*Nigerian Context*
NIST	National Institute of Standards and Technology	*Standards Body*
NITDA	National Information Technology Development Agency	*Nigerian Context*
NITDA-CERRT	NITDA Computer Emergency Readiness and Response Team	*Nigerian Context*
NLP	Natural Language Processing	*AI Security*
NSA	National Security Agency (United States)	*Standards Body*
O		
OAuth	Open Authorisation	*Identity & Access*
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	*Risk Management*
OIDC	OpenID Connect	*Identity & Access*
OS	Operating System	*Infrastructure*
OTP	One-Time Password	*Identity & Access*

Acronym	Full Meaning	Category
OWASP	Open Worldwide Application Security Project	*Application Security*
P		
PAM	Privileged Access Management	*Identity & Access*
PCI DSS	Payment Card Industry Data Security Standard	*Framework / Standard*
PKI	Public Key Infrastructure	*Cryptography*
PQC	Post-Quantum Cryptography	*Post-Quantum Cryptography*
Q		
QKD	Quantum Key Distribution	*Post-Quantum Cryptography*
QSC	Quantum-Safe Cryptography	*Post-Quantum Cryptography*
R		
RBAC	Role-Based Access Control	*Identity & Access*
RDP	Remote Desktop Protocol	*Network Security*
RFC	Request for Comments	*Standards Body*
RMF	Risk Management Framework	*Risk Management*
RPO	Recovery Point Objective	*Business Continuity*
RSA	Rivest-Shamir-Adleman (cryptographic algorithm)	*Cryptography*
RTO	Recovery Time Objective	*Business Continuity*
S		
SAST	Static Application Security Testing	*Application Security*
SDLC	Software Development Lifecycle	*Application Security*
SIEM	Security Information and Event Management	*Security Monitoring*
SIM	Subscriber Identity Module	*Telecommunications*
SLA	Service Level Agreement	*Governance*

Acronym	Full Meaning	Category
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm (FIPS 205)	*Post-Quantum Cryptography*
SoA	Statement of Applicability	*Governance / Audit*
SOC	Security Operations Centre (also: System and Organization Controls in SOC 2 context)	*Security Monitoring*
SP	Special Publication (NIST)	*Standards Body*
SSH	Secure Shell	*Network Security*
SSO	Single Sign-On	*Identity & Access*
SSRF	Server-Side Request Forgery	*Application Security*
T		
TDE	Transparent Data Encryption	*Data Protection*
TLS	Transport Layer Security	*Cryptography*
TTP	Tactics, Techniques, and Procedures	*Threat Intelligence*
U		
UEBA	User and Entity Behaviour Analytics	*Security Monitoring*
UPS	Uninterruptible Power Supply	*Physical Security*
V		
VAPT	Vulnerability Assessment and Penetration Testing	*Vulnerability Management*
VPN	Virtual Private Network	*Network Security*
W		
WAF	Web Application Firewall	*Application Security*
WebAuthn	Web Authentication	*Identity & Access*
WoG	Whole of Government	*Nigerian Context*
WPA3	Wi-Fi Protected Access version 3	*Network Security*
X		
XSS	Cross-Site Scripting	*Application Security*
Z		
ZTNA	Zero Trust Network Access	*Network Security*

DRAFT