REVISED ICT GUIDELINES FOR PENSION FUND OPERATORS

August 2025

Table of Contents

DEFINITION OF TERMS

S/No	TERM	DEFINITION
1	The Commission	The National Pension Commission.
2	Pension Fund Administrator	A corporate entity licensed by the Commission to manage pension funds and assets.
3	Pension Fund Custodian	A company licensed by the National Pension Commission to hold all pension funds and assets in safe custody on trust for holders and beneficiaries of Retirement Savings Accounts.
4	Closed Pension Fund Administrator	A Closed Pension Fund Administrator means an employer or its subsidiary licensed by the Commission to operate and exclusively manage any pension scheme as a Pension Fund Administrator.
5	Pension Fund Operator	Pension Fund Operators refer to Pension Fund Administrators, Closed Pension Fund Administrators and Pension Fund Custodians licensed by the National Pension Commission to carry out pension business.
6	Pension Fund	A pool of savings accumulated during the working life of employees and to be paid out as pension when they retire.
7	Employer	Any person or organisation that employs people (employees).

ABBREVIATIONS

S/No	ABBREVIATION	MEANING
1	PenCom	National Pension Commission “the Commission”
2	ICT	Information and Communication Technology
3	PFA	Pension Fund Administrator
4	PFC	Pension Fund Custodian
5	PFO	Pension Fund Operator
6	ISO	International Organization for Standardization
7	AI	Artificial Intelligence
8	RSA	Retirement Savings Account
9	SOP	Standard Operating Procedure
10	SLA	Service Level Agreement
11	UAT	User Acceptance Test
12	SAN	Storage Area Network
13	HTTPS	Hyper Text Transfer Protocol Secure
14	OS	Operating System
15	OEM	Original Equipment Manufacturer
16	SDLC	Software Development Life Cycle
17	API	Application Programming Interface
18	VAPT	Vulnerability Assessment and Penetration Testing
19	MFA	Multi-Factor Authentication
20	ISPs	Internet Service Providers
21	MTD	Maximum Tolerable Downtime
22	CAB	Change Advisory Board

SECTION 1: Introduction

1.0 General

The "ICT Guidelines for Pension Fund Operators (PFOs)" in Nigeria provides a crucial framework for technology adoption and operations in the pension industry. These guidelines aim to maintain consistency among operators and ensure their adherence while prioritising the security of information assets.

The National Pension Commission has prepared these ICT guidelines for Licenced PFOs to be used as minimum requirements and as appropriate to align with each operator’s technology adoption.

1.1 Scope

These guidelines aim to establish a minimum industry-wide standard for PFOs in Nigeria and apply to all electronically generated, received, stored, printed and scanned information within PFO operations.

These guidelines cover ICT governance and policy, ICT operations management, ICT infrastructure, business applications, information security, disaster recovery, business continuity planning, emerging technology adoption, service provider management and ICT mergers and acquisitions.

Strict adherence to these guidelines will enhance the operations of PFOs, protect customer information and contribute to the overall development and stability of the Nigerian pension industry.

1.2 Objectives

The objectives of these guidelines are:

i. To standardize the use and adoption of ICT practices across the pension industry for PFOs in Nigeria;
ii. To Identify, control and mitigate information system risks;
iii. To improve service delivery and ensure prompt retirement benefit payments;
iv. To raise awareness of stakeholders' roles in protecting information and digital assets;
v. To ensure the safety of information across the industry and guarantee data privacy; and
vi. To promote a roadmap to support digital transformation.

SECTION 2: ICT Governance & Strategy

2.1 Governance

2.1.1 The Board of PFOs shall ensure that adequate internal governance and internal control frameworks are in place for ICT functions.

2.1.2 PFOs shall set clear roles and responsibilities for ICT functions, information security and business continuity.

2.1.3 The PFO shall establish an ICT Management Committee comprising its Senior/Executive Management.

2.1.4 The ICT Management Committee shall have overall accountability for implementing the PFOs ICT Strategy and ensure it aligns with the Corporate Strategy.

2.2 Strategy

2.2.1 PFOs shall develop and execute an effective ICT Strategy.

2.2.2 The ICT Strategy shall align with the PFOs Corporate Strategy to promote technology integration and innovations.

2.2.3 The Board of the PFOs shall approve the ICT Strategy.

2.2.4 PFOs shall ensure regular monitoring and reporting of the implementation of the ICT Strategy to ensure the successful attainment of the Corporate Strategic objectives.

2.3 ICT Policies

2.3.1 PFOs shall document key ICT policies related to their operations.

2.3.2 ICT Policy documents shall establish general requirements and responsibilities for protecting ICT systems, covering standard technologies and undergoing regular review and updates.

2.3.3 ICT Policies shall ensure the implementation of appropriate controls, awareness programs and regular updates to protect the PFOs' ICT systems and address industry changes.

2.3.4 The Boards of the PFOs shall approve all ICT Policies.

2.3.5 PFOs shall have policies that define, but are not limited to the following:

- Technology Acceptable Usage
- Software Acquisition and Development
- ICT Asset Acquisition and Disposal
- Hardware and Software Maintenance
- Information and System Security
- Backup and Recovery
- Website and Intranet Management
- Cloud Operations
- Change Management
- Cyber Security
- Business Continuity Management
- Vendor Management
- Database Management
- Data Retention
- Email Usage
- Network Security
- Password
- Data Classification
- Data Protection
- Remote Access
- Bring Your Own Device (BYOD) (where applicable)
- Mobile Device Usage
- Virtualization
- API Management (where applicable)
- The use of Emerging Technology (where applicable)

2.4 Standard Operating Procedure (SOP)

2.4.1 PFOs shall develop and maintain a comprehensive set of SOPs that cover all critical ICT business processes.

2.4.2 The SOPs shall be documented in a clear, concise and easily understandable manner and should be updated regularly.

2.4.3 PFOs shall document all operational dependencies and their relationships in the SOP.

2.5 ICT Audit Controls

2.5.1 ICT Audit shall be tailored to the specific needs and requirements of the PFO, considering industry standards, regulatory requirements and the organization’s risk profile.

2.5.2 Audit on ICT functions shall follow a risk-based approach.

2.5.3 The ICT Internal Auditor shall independently review and provide objective assurance to the PFOs Management on the level of compliance with all ICT and security-related activities.

2.5.4 PFOs shall conduct both internal and external ICT audits at least once a year to identify and mitigate risks and vulnerabilities.

2.5.5 PFOs shall take appropriate measures to address the recommendations made in its ICT Audit Reports.

2.5.6 The ICT audit reports shall be presented to the Commission's Examination Officers during routine examinations.

2.6 ICT Security Risk Management

2.6.1 PFOs shall identify and manage their ICT security risks.

2.6.2 The oversight and management of ICT security risks shall be carried out by a Business Unit or Department within the PFO, distinct from ICT Department.

2.6.3 The Unit or Department responsible for ICT security risk management shall be responsible for monitoring, measuring and controlling vulnerabilities and threats to the PFO's ICT.

2.6.4 The ICT function(s) responsible for managing ICT systems, processes and security operations shall have appropriate procedures and controls to ensure all risks are identified, analysed, measured, monitored, managed, reported and kept within the PFO's risk appetite.

2.6.5 PFOs shall ensure that the ICT security risks are documented and continuously mitigate upon based on 'lessons learnt' during its implementation and monitoring process.

2.6.6 PFOs' Risk Management Framework shall contain a Section on ICT Security Risk adequately documented and approved by the Board.

SECTION 3: ICT Operations Management

ICT Operation Management comprises change, patch, incident, and asset management.

3.1 Change Management

3.1.1 PFOs shall establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner.

3.1.2 All changes on business applications implemented in the production environment must be governed by a documented process with necessary change details in line with the PFOs Change Management Policy.

3.1.3 The PFOs ICT Change Advisory Board (CAB) or Committee shall approve all changes to its information systems.

3.1.4 User Acceptance Test (UAT) for changes and upgrades to critical business applications shall be carried out and signed off by stakeholders before deployment.

3.1.5 The test environment must be separated from the production environment.

3.2 Patch Management

3.2.1 PFOs shall develop and maintain a Patch Management procedure.

3.2.2 A mechanism must be in place to regularly check for the availability of patches and ensure that all systems are patched and updated promptly.

3.2.3 The PFOs ICT Change approving authority must approve all patches before implementation in the production environment. A rollback mechanism should be in place to take care of patch failures.

3.3 Incident Management

3.3.1 PFOs shall establish and implement an incident management process to monitor and log operational and ICT security incidents. This incident management process shall enable PFOs to promptly continue or resume critical business functions and operations when disruptions occur.

3.3.2 The incident management process shall establish procedures to identify, track, log, categorise and classify incidents according to preset priorities based on business criticality, the roles and responsibilities for different incident scenarios and effective internal communication plans, including incident notification and escalation procedures.

3.3.3 All critical ICT incidents must be reported to the Commission within 72 hours of their occurrence.

3.4 Asset Management

3.4.1 PFOs shall maintain an up-to-date inventory of their ICT assets including ICT hardware and software, network devices, databases, etc.

3.4.2 The ICT asset inventory shall store the configuration of the PFOs ICT assets and the links and interdependencies between the different ICT assets to enable a proper design and change management process.

3.4.3 PFOs ICT asset inventory shall be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help respond to security and operational incidents, including cyber-attacks.

3.4.4 All data on ICT systems and associated storage devices shall be destroyed or overwritten before sale, disposal or reissue.

3.4.5 PFOs shall create and maintain a formal process for retiring assets that no longer meet performance requirements.

SECTION 4: ICT Infrastructure

4.1 Servers

The minimum server hardware requirements for PFOs shall be based on their specific operational needs, workload and growth projections to ensure optimal performance, reliability and security.

4.1.1 PFOs shall deploy a physical or virtual server with adequate resources.

4.1.2 PFOs shall deploy enterprise-grade server hardware to host applications and databases for reliability and performance.

4.1.3 PFOs may implement a server virtualisation strategy to optimise resource usage.

4.1.4 PFOs shall harden server configurations to minimise cyber-attacks.

4.2 Storage

4.2.1 PFOs shall deploy a scalable storage system.

4.2.2 The storage system may utilise a Storage Area Network (SAN) for Core applications, Databases and fileservers.

4.2.3 The storage system shall have inbuilt redundancy solutions to protect against data loss.

4.3 Data Center

4.3.1 The Data Center shall be a restricted area to which unauthorised access is denied. Access and visitor logs with dates and times should be maintained to record who has access to the Data Center.

4.3.2 The Data Center environment shall meet the minimum requirements for secured environmental control, adequate power and cooling capacity, and proper monitoring of fire, smoke and other hazards.

4.4 Network Infrastructure

4.4.1 PFOs shall plan and design their network topology/diagram based on business size and operational demands to ensure a secure and reliable network infrastructure.

4.4.2 PFOs shall deploy network devices (switches, routers and firewalls) with redundancy.

4.4.3 **The network devices shall have the capacity to be managed centrally, monitor the network and internet traffic**

4.5 Database

4.5.1 PFOs shall deploy a database management system that is scalable and proportional to their business needs.

4.5.2 PFOs shall maintain a “single point of truth” database that is resilient and capable of managing the integrity of the information generated at any time.

4.6 Operating System

PFOs Operating System (OS) minimal security and access control requirements may vary per OS and organisation.

4.6.1 PFOs shall use a supported and secure server operating system (e.g., Windows Server, Linux, etc).

4.6.2 The OS shall support multi-factor login.

4.6.3 The version of the OS must be within an OEM-supported life cycle.

4.6.4 The OS must have valid licenses.

4.6.5 The OS shall have built-in controls to restrict access to unauthorised personnel, both when on the domain and not on the domain, to protect sensitive data and prevent unauthorised users from making changes to the system.

4.7 Virtualisation

For PFOs utilising virtualised environments, the following shall be observed:

4.7.1 The PFOs shall configure virtualised environments to share centralised storage to achieve consolidated resource management.

4.7.2 PFOs shall implement enhanced security for the virtualised environment and an effective log management practice.

4.7.3 PFOs shall ensure that the virtual machines have a similar security policy as the physical servers under Section 4.1.

SECTION 5: Business Applications and Acquisition

5.1 Applications Development

5.1.1 PFOs shall use business applications to streamline operations, ensure compliance, improve customer service and make better decisions by achieving these baseline standards.

5.1.2 PFOs shall adopt the Software Development Life Cycle (SDLC) methodology with User Acceptance Test (UAT) in developing bespoke Applications.

5.1.3 The relevant business units/departments must conduct and sign off on the User Acceptance Test before the application’s go live.

5.1.4 Source Codes must be available and kept secure for in-house developed applications.

5.1.5 Documentation of the software shall be available and safely stored. The document shall, at minimum, contain the following:

i. Functionality in line with user requirements
ii. Security features
iii. Interface requirements with other systems
iv. System Documentation
v. Installation Manual
vi. User Manual
vii. UAT Report(s)

5.2 Application

5.2.1 PFOs shall ensure that ALL Pension-related software(s) deployed have the functionality to handle, but not limited to, the following:

i. Registration
ii. Collection
iii. Investment
iv. Administration
v. Fund Accounting
vi. Fund Performance
vii. Compliance Monitoring
viii. Risk Management
ix. Return Rendition
x. Document Management
xi. Customer Service, including Mobile Application
xii. Business Intelligence/Reporting.

5.3 Application Integration/Interfacing

5.3.1 PFOs shall ensure that all the Pension-related Software share data and functions to improve efficiency and allow interaction between different Software Applications (where applicable and practicable based on the Information required).

5.3.2 PFOs shall ensure that the Pension-related Software can interface with the Commission's applications, where required.

5.3.3 PFOs shall ensure that the Pension-related Software can integrate with PFAs (in the case of PFC) and PFC (in the case of PFA) in a secured manner using controlled Application Programming Interfaces (APIs).

SECTION 6: Information Security

PFOs shall develop and document an information security policy that shall define the high-level principles and rules to protect the Confidentiality, Integrity and Availability of RSA holders' information as well as PFOs information assets from vulnerabilities and threats.

6.1 Information Security Standards

6.1.1 PFOs shall work towards adopting Information Security Standards in line with globally recognised Security Management Standards ISO 27001:2013 or later, depending on their needs/structure.

6.1.2 **All PFOs shall attain the latest ISO 27001 certification within two (2) years of the effective date of implementation of these guidelines.**

6.2 Cybersecurity

Without prejudice to section 6.1, PFOs shall have the following minimum standards for information security:

6.2.1 Establish a cybersecurity programme to protect digital assets;

6.2.2 Deploy network security solutions to promptly manage vulnerabilities, detect threats and ensure collection of threat intelligence;

6.2.3 Maintain threat event log; and

6.2.4 Conduct external Vulnerability Assessment and Penetration Testing (VAPT) at least once a year.

6.3 Logical Security

6.3.1 PFOs shall manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including remote access.

6.3.2 Users (including technical users) shall be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').

6.3.3 PFOs shall implement Multi-Factor Authentication (MFA) on critical applications.

6.3.4 PFOs shall, at a minimum, ensure that all activities by privileged users are logged and monitored. Access logs shall be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets and following the retention requirements set out in the PFOs' access control policies.

6.3.5 PFOs shall ensure that applications deployed do not allow the same person to be both maker and checker of the same transaction.

6.4 Virus Protection

6.4.1 PFOs shall deploy ONLY licensed enterprise antivirus software on all systems.

6.4.2 Antivirus software shall be enabled for automatic scans and real-time protection to prevent threats.

6.5 Internet Service and Security:

6.5.1 All internet connections shall be routed through a firewall for systems connected to the network.

6.5.2 PFOs shall use HTTPS, update web browsers and educate employees about online threats like phishing etc.

6.5.3 PFOs shall maintain two Internet Service Providers (ISPs) for redundancy.

6.6 Information Security Training & Awareness

6.6.1 PFOs shall establish periodic information security training/awareness programmes for all its staff and contractors to ensure they are adequately trained on what to look out for as they perform their duties and responsibilities. This should be consistent with relevant security policies and procedures to reduce human error, theft, fraud, and misuse, as well as address information security-related risks.

6.6.2 PFOs shall ensure that the training/awareness programme is conducted at least twice a year to all staff members and contractors.

SECTION 7: Business Continuity and Disaster Recovery

PFOs shall establish a sound Business Continuity Management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption.

These following provide a minimum framework for PFOs to ensure ICT systems' resilience and operations' continuity during adverse events:

7.1 Business Impact Analysis (BIA)

7.1.1 PFOs shall conduct a comprehensive Business Impact Analysis (BIA) to identify critical ICT systems, applications and data vital for business operations.

7.1.2 It is imperative that the Maximum Tolerable Downtime (MTD) shall be determined for each critical system to prioritise recovery efforts appropriately.

7.1.3 PFOs shall ensure that their ICT systems and ICT services are designed and aligned with their BIA, with redundancy of critical components to prevent disruptions caused by events impacting those components.

7.2 ICT Disaster Recovery Plan (DRP)

7.2.1 PFOs shall develop a detailed ICT Disaster Recovery Plan (DRP) that outlines step-by-step procedures to restore ICT services after a disruption. This ICT DRP must align with the PFOs BCM Plan.

7.2.2 A Disaster Recovery Site (DRS) must be in place to replicate the Data Center (Production Site).

7.2.3 PFOs shall regularly review and test the recovery plan to ensure its effectiveness and identify areas for improvement.

7.2.4 The location of an alternate DR site shall be based on a documented risk assessment and a minimum Tier III Data Center standard.

7.3 Redundancy and Failover

7.3.1 PFOs shall Implement redundant ICT systems, such as servers, storage, and network components, to ensure high availability for business-critical applications and minimise single points of failure.

7.3.2 PFOs shall use failover mechanisms to switch to redundant systems automatically in case of primary system failure.

7.4 Data Backup and Replication

7.4.1 PFOs shall regularly back up critical data and store backups securely in off-site or cloud locations.

7.4.2 PFOs shall consider real-time data replication for critical systems to ensure minimal data loss during a disruption.

7.4.3 PFOs shall periodically perform a restore of selected data from previously backed-up data on tape to check the integrity of data stored on them. This exercise is to be done at least quarterly with documented evidence.

7.5 Employee Training and Awareness

7.5.1 PFOs shall train employees on their roles and responsibilities during a business disruption.

7.5.2 PFOs shall conduct regular drills and simulations to ensure employees are familiar with the recovery procedures.

7.6 Vendor and Supplier Management

7.6.1 PFOs shall evaluate critical vendors' and suppliers' business continuity plans to ensure they can continue to provide essential services during disruptions.

7.6.2 PFOs shall maintain a list of alternative vendors that can be engaged if primary suppliers are unavailable.

7.7 Testing and Exercises

7.7.1 PFOs shall conduct annual business continuity tests and exercises to validate the plan's effectiveness and identify areas of improvement. This may be conducted twice yearly to provide extra assurance.

7.7.2 PFOs must document lessons learnt from each test/exercise and use them to refine the plan.

7.8 Review and Maintenance

7.8.1 PFOs shall review and update the BCP at least once a year to reflect changes in the organization’s infrastructure, personnel and business processes.

7.8.2 PFOs must ensure that contact lists, recovery procedures and other critical information are up to date.

SECTION 8: Emerging Technology Adoption

8.1 Cloud Service

PFOs can host data on the cloud with the approval of the Commission and in line with the Nigeria Cloud Computing Policy.

Hosting information on the cloud does not absolve PFOs of their data integrity, confidentiality and availability responsibilities. The following minimum requirements apply to cloud computing:

8.1.1 Data hosted on the cloud must comply with extant Nigerian laws and regulations on Data Privacy and Data Sovereignty.

8.1.2 PFOs must define control requirements for the data to be hosted on the cloud.

8.1.3 PFOs shall apply the Zero Trust principle where applicable for cloud implementation

8.1.4 PFOs shall assess the risk impact on Business Continuity and Disaster Recovery plans before using cloud service.

8.1.5 The contract or Service Level Agreement (SLA) for cloud hosting must clearly define the control requirements.

8.1.6 PFOs shall avoid vendor lock-in when adopting a cloud model to host its services.

8.2 Artificial Intelligence (AI)

These guidelines aim to promote responsible and beneficial deployment of AI in the PFO, emphasising ethics, privacy, compliance, human involvement and ongoing evaluation.

The following should be adopted for the Use of Artificial Intelligence (AI):

8.2.1 Deployment of AI shall adhere to ethical principles such as transparency, fairness and accountability.

8.2.2 PFOs must protect personal data and ensure robust security measures against unauthorised access or misuse are put in place.

8.2.3 PFOs should comply with relevant laws, regulations and industry standards governing the use of AI and robotics in the pension industry.

8.2.4 Regular monitoring and evaluation of AI and robotics systems should be conducted to ensure accuracy, effectiveness and compliance with objectives.

8.2.5 PFOs should actively engage stakeholders, including pensioners and employees, to address concerns, provide transparency and foster trust in AI and robotics.

8.3 Mobile Devices

To mitigate the risks posed by mobile devices, operators shall consider putting additional controls in place to prevent data leakage. The following are the minimum controls for the benefit of mobile devices:

8.3.1 PFOs shall ensure mobile devices connected to the network are authenticated.

8.3.2 Two (2) Factor Authentication shall be applied to all mobile devices.

8.3.3 PFOs shall limit the synchronisation of sensitive data.

8.3.4 PFOs must enforce encryption of data with an on-device key for local backups.

8.3.5 PFOs shall disable or encrypt removable media for all critical data access.

8.3.6 There shall be a procedure for remote access for mobile devices.

8.3.7 A data wipe procedure shall be established and enforced in case of theft or loss of a mobile device containing critical information.

8.4 Social Media

8.4.1 PFOs shall establish appropriate policies, processes and technologies to ensure that communications through social media platforms that may be impacted by litigation or regulations are tracked, monitored and archived appropriately.

8.4.2 Operators shall manage accessibility to social media sites through content filtering or by limiting network throughput to social media sites.

SECTION 9: Service Provider Management

9.1 Service Level Agreement (SLA)

PFOs shall set clear expectations, provide assurance to customers and ensure high service quality and accountability. SLAs shall be developed to support managing customer relationships, resolving issues and improving service delivery.

9.1.1 SLAs shall clearly define the scope of service and the overall objectives to be achieved.

9.1.2 The SLAs shall outline the specific services the PFO provides and the corresponding performance targets or metrics.

9.1.3 The SLAs shall establish agreed-upon service levels and associated penalties or incentives based on performance. These penalties and incentives are motivators to ensure compliance with the agreed-upon service levels.

9.1.4 The SLAs shall specify the frequency of review and the process for amendments or updates to the agreement.

9.1.5 All SLAs MUST be sent to the Commission for review, input and approval before they are executed.

9.2 Outsourcing of ICT Services

9.2.1 Outsourcing activities and services to vendors must be evaluated based on the following criteria:

i. The objective behind outsourcing.
ii. The economic viability.
iii. The risks and security concerns must be evaluated and mitigated.
iv. An escrow account shall be maintained with third parties in the event of the vendor's bankruptcy for software acquisition.

9.3 Shared Service Agreement

9.3.1 PFOs may engage in shared services if they need more expertise and capacity to perform these services.

9.3.2 PFOs may, with the Commission's approval, enter into a Shared Services Agreement on information security and other IT Services with their parent company.

9.3.3 PFOs must implement policies and procedures to ensure the independence and effectiveness of shared services. These policies shall be submitted to the Commission and must include the following minimum requirements:

i. Detailed description of the shared services to be provided.
ii. A clear indication of how the services will be shared, including the roles and responsibilities of the relevant or parties involved.
iii. A methodology for pricing shared services, including standards for timely recording and settlement and a specified payment frequency.
iv. Specify a governance structure for reporting exceptions to policy and an annual review of the shared services policies.
v. PFOs shall allocate technology acquisition costs based on the services they use.
vi. PFOs with foreign parent companies shall ensure their technology transfer agreements allow them to use the technology for their benefit.
vii. All transactions between service providers and PFOs, including shared service fees, must be appropriately documented with contracts, invoices and other relevant documents as evidence.
viii. An independent consultant's examination of the fees and services delivered shall be submitted to the Commission annually, demonstrating conformity with existing rules and regulations.

SECTION 10: ICT Merger & Acquisition

The harmonisation of ICT processes during mergers and acquisitions is crucial to maximise synergies and ensure the realisation of the expected value from the acquisition. The integration of ICT acquisition involves combining the acquired business's ICT operations, services and systems with those of the acquirer.

The following are the minimum requirements for successful ICT integration during mergers and acquisitions:

10.1 Consideration shall be given to necessary changes in the existing ICT infrastructure when integrating with the acquirer.

10.2 The Change Advisory Board must thoroughly document and approve all integrations.

10.3 PFOs shall assess their internal resources and determine if additional support from an outsourcing provider is needed.

10.4 The acquiring PFO must provide a clear and approved implementation plan, which shall be transparent and free from hidden or undisclosed information, as reviewed and approved by the Commission.

10.5 Both parties shall conduct an ICT risk assessment for a successful ICT integration during mergers and acquisitions. The final risk assessment report shall be submitted to the Commission for approval.

10.6 PFOs shall define well-outlined roles and responsibilities for all technical teams participating in the IT integration process during mergers and acquisitions.

SECTION 11: Effective Date

These Guidelines take effect from 1st January, 2025.

SECTION 12: Review and Enquiries

These Guidelines shall be subject to review by the Commission from time to time as the need arises.

All enquiries regarding these Guidelines should be directed to the Director-General, National Pension Commission.

GLOSSARY OF TECHNICAL TERMS AND DEFINITIONS

S/NO	TERM	DEFINITION
1	ISO 27001/27002	ISO 27001 and ISO 27002 are two internationally recognised standards that provide information security management systems (ISMS) guidelines
2	Cybersecurity	the protection of internet-connected systems such as hardware, software and data from cyber threats
3	Database	organised collection of structured information or data, typically stored electronically in a computer system
4	Data Center	a facility composed of networked computers and storage used to organise, process, store and disseminate large amounts of data
5	Information Security	the process of protecting sensitive information from unauthorised activities, including inspection, modification, recording and any disruption or destruction
6	Social Media	refers to interactions among people in which they create, share and/or exchange information and ideas in virtual communities and networks.
7	Service Level Agreement (SLA)	SLA is a contract between a service provider and its customers that describes the products or services to be delivered. The contract also highlights the terms and conditions as well as the responsibilities of the parties.
8	Servers	specialized computers or software applications designed to manage network resources and provide services to other computers (referred to as clients) in the network

9	Mobile device	a piece of portable electronic equipment that can connect to the internet, such as a laptop computer, tablet or smartphone
10	Outsourcing	is a business practice in which services or job functions are hired out to a third party on a contract or ongoing basis.
11	Data Backup	is the process of making a copy of your digitized data and other business information in case your data is damaged, deleted or lost.
12	Multifactor Authentication	is a security measure designed to enhance the protection of digital accounts and systems by requiring users to provide multiple forms of identification before granting access.
13	Business Continuity/Disaster Recovery	Describes the ability of an organization to maintain essential functions during and after a disaster has occurred.
14	Disaster Recovery Plan	a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber-attacks and any other disruptive events
15	Failover	is the ability to switch automatically and seamlessly to a reliable backup system.
16	Virus	a type of malicious software, or malware, that spreads between computers and causes damage to data and software.
17	Virtualisation	Virtualisation is the process of creating a virtual version of something, including servers, storage devices, network resources and operating systems.
18	Risk Management	refers to the process of identifying, assessing and mitigating the potential risks associated with using technology and information systems within an organization.

19	Change Management	a systematic approach to dealing with the transition or transformation of an organisation's goals, processes or technologies.
20	Change Advisory Board	refers to a group of people (technical staff and crucial business decision makers) who are responsible for reviewing, assessing impact and approving ICT changes.
21	Patch Management	is the process of applying updates to software, drivers and firmware to protect against vulnerabilities.
22	Incident Management	the process used by organisations to respond to an unplanned event or service interruption and restore the service to its operational state.
23	Asset Management	is the process of planning and controlling the acquisition, operation, maintenance, renewal and disposal of organisational assets.
24	Data Replication	a method of copying data to ensure that all information stays identical in real time between all data resources.
25	Cloud Computing Service	is a method of delivering Information and Communication Technology (ICT) services where the customer pays to use, rather than own its resources such as Infrastructure (hardware), Databases and Software.
26	Emerging Technology	refers to new and innovative technologies that are being developed or have recently been introduced into the market.