Nigerian Financial Services Industry

IT Standards Blueprint for Payment Service Providers (PSPs) and National Microfinance Banks (NMFBs)

Version 1.0

August 2021

PREAMBLE

This IT Standards Blueprint document presents the framework for the adoption of Information Technology (IT) Standards for the Payment Service Providers and National Microfinance Banks in the Nigerian Financial Industry.

This document encourages Financial Institutions in Nigeria to develop, grow and sustain competency in Information Technology. It hopes to achieve this by serving as a framework and guide for the use of and implementation of Information Technology and Information Technology (IT) Standards. The overall objective is to bring Nigerian Financial Institutions to an acceptable minimum level of process maturity, which will help drive sustainable growth, build resilience and improve customer experience.

This document contains the IT Capability areas selected for Financial Institutions to develop competency as well as the rationale for inclusion of the Capability area in the Blueprint. It also contains Standards recommended for building proficiency and developing competence in the IT Capability areas. For each defined Standard, the documentation includes the objective and intention, description, minimum acceptable maturity level, derivable benefits, requirements for compliance, and consequences for deviations.

This document is the property of the Central Bank of Nigeria (CBN) and its usage is restricted to members of the Shared Services Office, the IT Standards Council, and Nigerian Financial Services Industry and authorized accredited third-party agents or consultants as the CBN deems fit.

For questions and clarifications, please contact the IT Standards Council through the following:

Deputy Governor Operations
Central Bank of Nigeria
Central Business District
Abuja
Attn: Shared Services Office

Table of Contents

List of Tables and Figures

Abbreviations

ITCMM	IT Capability and Maturity Model
ITIL	IT Infrastructure Library
ISACA	Information Systems Audit and Control Association
XBRL	eXtensible Business Reporting Language
CMMI	Capability Maturity Model Integration
SPICE	Software Process Improvement and Capability Determination
SCAMPI	Standard CMMI Appraisal Method for Process Improvement
PMI	Project Management Institute
PMBOK	Project Management Body of Knowledge
PRINCE2	Projects IN Controlled Environments version 2
TIA	Telecommunications Industry Association
BCI	Business Continuity Institute
PCI DSS	Payment Card Industry Data Security Standard
SFIA	Skills Framework for the Information Age
IPA	Intelligent Process Automation
ISO	International Organization for Standardization

1 INTRODUCTION

1.1 Background

Globally, Financial Institutions depend on Information Technology (IT) to help them achieve their vision, and strategy. IT has transformed the ways Financial Institutions operate, their products and how they interact with customers. IT plays an important role in product innovation, gaining market advantage, operational efficiency and communicating in the global market place. Indeed, Information Technology is strategic for the continual existence and success of the Financial Services Industry in Nigeria.

Over the past 20 (twenty) years, there has been a consistent increase in IT investments by Nigerian Financial Services Institutions. The investments are driven by several factors, including evolving business needs and regulatory mandates. However, commensurate value is not realized from these investments due to:

- Low level of organisational maturity in terms of processes and people
- Lack of executive management commitment and support
- Cultural resistance to (technology) change
- Non-Standard systems and infrastructure
- Low level of technology awareness
- Cyber crime
- Lack of qualified and skill personnel to run and manage IT resources
- Inadequate research on market needs before investment in IT products

To address these gaps and provide a framework and point of reference for the utilisation of Information Technology, the IT Standards Council of the Central Bank of Nigeria developed and published the IT Standards Blueprint for Nigerian Financial Services Institutions.

The IT Standards Blueprint for PSPs and National MFBs became published in year 2021 to have a standardized and secure eco-system within the financial industry

1.2 Inclusion of Payment Service Providers and National Microfinance Banks into the IT Standards Framework.

The Payment Service Providers (PSPs) and National Microfinance Banks(NFMBs) have now been integrated into the IT Standards framework to have an end-to-end operational standard across the financial services industry and reduce loopholes that may exist within the financial chain.

This document reviews standards and seeks ways to adapt them for the Payment Service Providers (PSPs) and National Microfinance Banks (NMFBs).

The proposed IT standards blueprints for the Payment Service Providers (PSPs) and National Microfinance Banks are sub-divided into three majors categories, namely:

- Service Management: This covers the quality of IT delivery between both providers and consumers of financial services. Some of the proposed standards include: ITILV4, Project Management (PRINCE2/PMBOK), and Business Continuity
- Interoperability and Cost Management: This covers aspects of technical interoperability with other financial bodies. The proposed standards are ISO 8583:2003, ISO 20022, eXtensible Business Reporting Language (XBRL), Open Banking - Open Banking Standard
- Security: This covers the protection of data and technology assets used within the financial sector, and some of the proposed standards are ISO 27001/27002, PCI-DSS, NDPR, and ISO 27032.

1.3 Objectives and Purpose of Document

This document presents Standards for Information Technology for the Nigerian Financial Services Industry. For each defined Standard, the documentation includes the following:

- Objective and intention
- Description of the Standards
- Benefits to Financial Service Institutions
- Requirements for compliance

Financial Service Institutions are expected to achieve and maintain compliance to the Standards listed in this Blueprint with the overall aim of attaining an acceptable minimum level of process maturity in the different capability areas.

The focus of the Blueprint is to drive and encourage process maturity within the Financial Services Industry rather than certification. Going through the certification process and obtaining certification to the Standards is not mandatory and will be assumed to be an extra above the minimum requirements defined in this blueprint.

1.4 Definition of Standard

For the purposes of this document, a Standard is an established, measurable and achievable set of requirements, methods, processes, practices and criteria agreed by general consent to be a basis of comparative evaluation.

1.5 Overview and Summary IT Standards for the Nigerian Financial Services Industry

The IT Standards Blueprint aims to help Nigerian Financial Services institutions develop capabilities under six (6) key technology Capabilities areas. Skills in these capability areas would support the

transformation of the Financial Institutions' IT function to a world class, high performing IT operations and help to position it as a strategic asset to the Financial Institution.

Capability Area	
Strategic IT Alignment	Translation of business vision and strategies into multi-year IT investments and operating plans as well as impacts of Information Technology on the Enterprise's performance measurement.
Architecture & Information Management	Guidance for the creation and execution of the strategic IT architecture framework
Solutions Delivery	Framework for the development of software application solutions and their subsequent transition into the production environment
Service Management & Operations	Planning, delivery and measurement of day-to-day operational service
Information & Technology Security	Security and protection of enterprise information and related assets
IT Innovation	Guidance on technology usage to create efficient organisations and improve alignment between technology initiatives and business goals.

Table 1: IT Capability Areas

The Financial Industry IT Standards are derived from globally defined and accepted Standards as follows:

Capability		Standards	
Strategic IT Alignment		IT Infrastructure Library (ITIL)	
Architecture & Information Management	Interfaces	ISO 8583	ISO 20022
	Reporting	eXtensible Business Reporting Language (XBRL) version 2.1	
Solutions Delivery	Project Management	Project Management Body of Knowledge (PMBOK)	Projects IN Controlled Environments version 2 (PRINCE2)
Service Management & Operations	Data Center	Uptime Institute's Tier Topology Standard:2018	ISO 22301 [1]
	Business Continuity	Business Continuity Institute Good Practice Guidelines (BCI GPG)	ISO 22301 [2]
Information & Technology Security	Payment Card Security	Payment Card Industry Data Security Standard (PCI DSS)	
	Information Security	ISO 27001/27002	
	Cyber Security	ISO 27032	
	Cloud Security	ISO 27017	
	Data Protection	NDPR	
IT Innovation	Open Banking	Open Banking Standard v3.1.2	

Table 2: IT Capability Areas and IT Standards

1.6 IT Standards Roadmap

The roadmap for IT Standards is presented below, indicating the standards that are due for compliance in 2022 and 2023.

			2022	2022	2022	2023	2023	2023
Capability Area		**Standards**	**March**	**June**	**Sept**	**March**	**June**	**Sept**
Strategic IT alignment	ITIL	ITILv4		▨				
Architecture & Information Management	Interfaces	ISO 8583 /	▨					
		ISO 20022				▨		
	Reporting	XBRL						▨
Solution Delivery	Project Management	PMBOK/						
		PRINCE2						▨
IT Operations	Business Continuity	BCI GPG/	▨					
		ISO 22301						
Information & Technology Security	PCI DSS , Info Sec.	PCI DSS	▨					
		ISO 27001/27002			▨			
	Cyber Security	ISO 27032						▨
	Data Protection	NDPR		▨				
	Cloud Security	ISO27017					▨	
IT Innovation	Open Banking	Open Banking Standards v3.1.2					▨	

▨ Initial Compliance Date

Figure 1: IT Standards Implementation and Adoption Timeline

1.7 Target Maturity Levels

Maturity levels indicate the robustness of formal articulation of policies and the extent of assimilation and adoption into organisational practices.

While the Blueprint encourages adoption of IT Standards, the focus is on process maturity and not on certification because process maturity provides Financial Institutions the opportunity to improve processes and embed global leading practices within the organisation resulting in tangible, visible improvements.

The definition of maturity levels is derived from common acceptable IT Standard models.

Level	Description	Characteristics of level
0	Non-existent	• No articulation of policies and recognisable processes are lacking
1	Ad-hoc	• Processes are not standardised, but ad-hoc approaches are applied incidentally on an individual or case-by-case basis • The overall approach to IT management and governance is improvised, impromptu and non-predictable
2	Repeatable	• Processes have evolved to the extent that similar approaches are adopted by different individuals undergoing the same task • There is no formal training or communication of Standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals
3	Defined	• Processes are properly defined and documented, and communicated through formal training • Processes are integrated into organisational practices via formal approved policy • Automation and tools are used in a limited and fragmented way
4	Managed and Measurable	• Measurable quality goals are established and management monitors and measures compliance with procedures and takes corrective action where processes appear not to be working effectively • Processes are under constant improvement and provide good practice
5	Optimised	• Processes are refined to the level of good practice, based on continuous improvement • Quality management & continuous improvement activities are embedded in process management • IT is leveraged in an integrated way to automate the workflow, providing tools to improve quality and effectiveness

Table 3: Definition of Maturity Levels

The target maturity level for IT Standards for the different categories of financial services institutions is detailed in the table below:

Category	Financial Services Institution	Maturity
Category One	• All Licensed National Microfinance Banks • All Licensed Payment Service Providers	Level 2

Table 4: Categorisation of Maturity Levels Across FSIs

Level 2 maturity requires that IT Standards are:

- Repeatable
- Partially Documented
- Given no formal training
- High degree of reliance on the knowledge of individuals

The table below provides the detailed explanation of the expectations of a level 2 process maturity for each Standard.

Categories	Description of Level 2 Maturity
Repeatable	• Some aspects of the process are repeatable because of individual expertise
Partially Documented	• There is a general assumed awareness of the existence of the processes • Some documentations and informal understanding of the processes exist • There is informal understanding of policies and procedures
Given no formal training	• Minimum skill requirements are identified for critical areas • Training is provided in response to needs, rather than on the basis of an agreed plan. • Informal training on the job occurs
High Degree of reliance on the knowledge of individuals	• Common approaches to use of tools exists but are based on solutions developed by key individuals. • An individual assumes his/her responsibility and is usually held accountable, even if it is not formally agreed. • Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelf ware.

Table 5: Description of Level 2 Maturity

2 IT Standards Blueprint

This section outlines the blueprint of the IT Standards and includes the following in respect of each Standard:

- Purpose of the Capability Area
- Justification/rationale for inclusion of this Capability area in the Blueprint
- Standard(s)
- Version of the Standard to which Compliance is Required
- Minimum Acceptable Maturity Level
- Description of the Standard(s)
- Rationale for Selection
- Benefits
- Requirements for compliance
- Scope
- Deviation from Use
- References

2.1 Strategic IT Alignment

Purpose	The Strategic IT Alignment Standards provide a framework for ensuring that business vision and strategies are translated into IT investments and operating plans.
Justification	**Business Challenge** • Misalignment between IT and business professionals • Difficulty in obtaining management buy-in for IT projects • Wrong impression that IT is not working **How this Capability Addresses these Challenges** Building capability in Strategic IT Alignment enables Financial Institutions develop: • A shared understanding of how IT applications, technologies and services will contribute to business objectives – today and in the future • A shared focus on where to expend scarce resources, time and money; the trade-offs the enterprise is prepared to make • A credible working relationship between the IT organisation and the rest of the business evidenced by reliable daily operations, responsive problem management and predictable, innovative solution delivery **Business Benefits** Outcomes of the strategic alignment of IT with the business include: • A good understanding of how emerging technologies, applications and trends can or will impact the Bank and its IT organisation • Clear expectations of IT, on how it will contribute to reaching the Financial Institution's business goals and objectives • Executive management support for IT initiatives • Support from key executives to participate in developing the IT Strategy • A well-articulated definition of IT's role in the Financial Institution's strategic (long term) plans • Effective use of IT to support enterprise goals & objectives which in turn delivers value to enterprise stakeholders and maximization of investment value
Standards	• IT Infrastructure Library (ITIL): globally adopted framework for IT Operations and Service Management
Version of the Standard to which Compliance is Required	• ITIL 4 2019
Minimum Acceptable Maturity Level	• Level 2

Rationale for Selection	**ITIL 4** The Service Strategy Volume of ITIL focuses on the alignment of business and IT so that each brings out the best in the other. It ensures that every stage of the service lifecycle stays focused on the business case and relates to all the companion process elements that follow. ITIL is also reference Standards for IT Governance and Service Management respectively
Benefits	• Standardized framework for ensuring that IT plans, and investments are directly driven by the business goals. • Ensures that IT services are designed to satisfy the business requirements and service levels • Objective basis for measuring the value IT brings to the business
Requirements for compliance	Adoption of the ITIL Service Strategy volume maturity level 2 The process for demonstrating compliance to ITIL is as follows: • Implement the IT Strategy requirements of the ITIL frameworks to the respective maturity level 2 and submit for a formal assessment by the IT Standards Council
Scope and Application	The Strategic IT Alignment Standard shall be applicable to all IT infrastructure and Service providers to the Financial industry including in-house Bank functions and external IT infrastructure and service providers
Exemption	Not applicable
References	ITIL: https://www.officialitil4.com/

2.2 Architecture and Information Management

2.2.1 Interfaces

Purpose	The purpose is to ensure the Standardization of transaction interfaces between entities in the Financial Services Industry to enhance interoperability and improve efficiency
Standards	• ISO 8583 also known as *Banking Transaction Card Originated Messages – Interchange Message Specifications*, provides a Standard framework for systems that exchange electronic transactions made using payment cards • ISO 20022 aims to enable communication interoperability between Financial institutions, their market infrastructures and their end-user communities by defining and promoting a single ISO Standardization approach to be used by all Banking Standards initiatives.
Version of the Standard to which Compliance is Required	• At least ISO 8583: 1987. Compliance to ISO 8583: 1993 and ISO 8583: 2003 also suffice • ISO 20022 – 1 2004
Maturity Level	• Level 2
Rationale for Selection	**ISO 8583** Standard framework for systems that exchange electronic transactions that use payment cards, specifies a common interface by which Banking transaction card originated messages may be interchanged between acquirers and card issuers. Most core Banking application vendors provide native ISO 8583 interfaces and **ISO 8583** is widely adopted within the Nigerian Financial Services industry for card-based payment transactions. **ISO 20022** Also known as the Universal Financial industry (UNIFI) message scheme provides a common platform for the development of messages in a Standardized XML syntax and is the de-facto Standard adopted in Europe to facilitate the Single Euro Payments Area (SEPA). ISO 8583 is restricted to card-based payments while the scope of application of ISO 20022 is broader.
Benefits	• Improved interoperability and efficiency of transaction processing • Cost savings due to interoperability • Facilitates straight through processing
	Transaction interfaces that meet specified industry Standards. **Process for compliance**

Requirements for compliance	• Implement the requirements of the interface Standards and submit to a formal assessment by the IT Standards Council. • If all requirements are met, the organisation will be deemed to have complied by the IT Standards Council
Scope	This Standard is applicable to all Financial Institutions, managed service providers and payments systems solution providers in the industry. • All organisations that provide payments services are required to provide ISO 8583 compliant interfaces. • Compliance with ISO 20022 requirements is mandatory.
Exemption	A payment service provider may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council

Key Elements of the Standards

ISO 8583:

Common interface by which Banking transaction card originated messages may be interchanged between acquirers and card issuers. It specifies message structure, format and content, data elements and values for data elements.

The specification has 3 parts:

- Part 1: Messages, data elements and code values
- Part 2: Application and registration procedures for Institution Identification Codes
- Part 3: Maintenance procedures for messages, data elements and code values

An ISO 8583 message is made of:

- Message type indicator (MTI)
- One or more bitmaps, indicating which data elements are present
- Data elements, the fields of the message

Ref: http://www.iso.org/

ISO 20022

Communication interoperability between Financial Services institutions, market infrastructure and end-users in respect of Banking transactions including:

- High value payments
- FX & Money Markets
- Commercial payments
- Cards
- Securities
- Trade

The ISO 20022 statement is organized as follows:

- Part 1: Overall Methodology and Format Specifications for Inputs and Outputs to/from the ISO 20022 Repository
- Part 2: Roles and responsibilities of the registration bodies
- Part 3: ISO 20022 Modeling
- Part 4: ISO 20022 XML design rules
- Part 5: ISO 20022 Reverse engineering
- Part 6: ISO 20022 Message Transport Characteristics

Ref: http://www.iso.org/

2.2.3 **Reporting**

Purpose	Standardization of business and Financial reporting across the industry
Justification	**Business Challenge** • Increase in transparency crisis in business transactions as a result of inability of stakeholder and auditors to have a common understanding of the scope of audit function and transparency needed during performance of audit work **How this Capability Addresses the business Challenge** • XBRL uses XML technologies to make the flow of Banking and business data more transparent and efficient • XBRL provides a standard platform for communication among all (local and global) stakeholders **Business Benefits** • The use of XBRL reduces the cost of capturing data, improves the timeliness, flexibility and quality of data collected and enables the easy reuse of data • XBRL supports executive leadership in making sound decisions by integrating business and IT planning, budgeting, standards, processes and governance which defines and maintains the company's operating environment. • Improves data quality and hence reduces work for both internal and external auditors by automatically checking the validity of the generated reports
Standards	• eXtensible Business Reporting Language (XBRL) version 2.1
Maturity Level	• Level 2
Version of the Standard to which	• XBRL 2.1

Compliance is Required	
Description of Standards	• XBRL is an XML-based open Standard for exchanging business information which allows information modeling and the expression of semantic meaning commonly required in business reporting.
Rationale for Selection	**XBRL** • XBRL provides a method to prepare, publish, exchange, search and analyze Banking statements across all software formats and technologies. • Includes an IFRS taxonomy which facilitates the electronic use and exchange of banking data in line with IFRS directives.
Benefits	• Improved reporting efficiency as data from various systems and databases are assembled quickly, cheaply and efficiently • Improved usability of Financial statement information • Simplification of both internal and external reporting processes
Requirements for compliance	To be compliant, an organisation must implement XBRL processes and tools and utilize it for reporting purposes. **Process for compliance** • Implement XBRL and submit to a formal assessment by the IT Standards Council • If all requirements are met, the organisation will be deemed to have complied by the IT Standards Governance Council
Scope	This Standard is applicable to all financial institutions and external (managed) service providers for the Financial Services industry.
Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council

Key Elements of the Standards

XBRL consists of an XBRL instance, containing primarily the business facts being reported, and a collection of taxonomies (called a Discoverable Taxonomy Set (DTS)), which define metadata about these facts, such as what the facts mean and how they relate to one another

- XBRL Instance: The XBRL instance begins with the <xbrl> root element and holds the following information:
    - Business Facts which are divided into two categories
        - Items are facts holding a single value. They are represented by a single XML element with the value as its content.
        - Tuples are facts holding multiple values. They are represented by a single XML element containing nested Items or Tuples.
    - In the design of XBRL, all Item facts must be assigned a context.
        - Contexts define the entity (e.g. company or individual) to which the fact applies, the period the fact is relevant, and an optional scenario. Scenarios provide

further contextual information about the facts, such as whether the business values reported are actual, projected, or budgeted.

- Units define the units used by numeric or fractional facts within the document, such as USD, shares. XBRL allows more complex units to be defined if necessary.
- Footnotes use XLink to associate one or more facts with some content.

- Taxonomy: An XBRL Taxonomy is a collection of taxonomy schemas and linkbases. A taxonomy schema is an XML schema file. Linkbases are XML documents which follow the XLink specification. The schema must ultimately extend the XBRL instance schema document and typically extend other published XBRL schemas.

Ref: www.xbrl.org

2.3 Solutions Delivery

2.3.1 Project Management

Purpose	The Project Management Standard provides a framework to guide project planning, organizing, and resource management to bring about the successful completion of project goals and objectives.
Justification	**Business Challenge** • High cost implication of annual implementation or modification of existing solutions to meet the demands of customers and align itself with the current realities in the environment • Disappointing returns on investment as a result of project failure **How this Capability Addresses these Challenges** • Enhances an organisation's competitive edge, by ensuring that organisations' project management strategies directly aligns with the strategic business goals. • Ensures standard processes are put in place to deal with all contingencies and that a minimum level of quality results that meets requirements and expectations is achieved. **Business Benefits** • Increases clarity of the project portfolio which will allow improvement in reviewing and culling of projects without clear business cases and stopping or re-scoping projects without a methodology • Guarantees that the right sequence of project activities are carried out by keeping track of the strategic objectives of the project, its intended business benefits and quality perspective throughout the lifespan of the project • Supports projects to follow timelines and meet deadlines which in turn reduces project cost, time spent modifying schedules and timelines and increases productivity • Improves project success rates by anticipating risks and providing guidance on how to avoid them

Standards	• Project Management Body of Knowledge (PMBOK): a global Standard in Project Management, developed by the Project Management Institute (PMI) which provides a set of Standard terminology and guidelines for project management • PRojects IN Controlled Environments (PRINCE2): a process-driven project management method, which is developed by the Office of Government Commerce (OGC), UK, and is largely influenced by the IT industry
Version of the Standard to which Compliance is Required	• PRINCE2 – 6th Edition (2017) • PMBOK Guide — Seventh Edition (2021)
Maturity Level	• Level 2
Rationale for Selection	**PMBOK** The PMBOK is a global Standard which establishes best practices and principles for project management. **PRINCE2** Prince2 is a widely adopted structured method for effective Project Management, which covers the management, control and organisation of a project Both Standards are independent Project Management Standards widely adopted both globally and locally.
Benefits	• Improved efficiency and effectiveness in project delivery • Better risk management • Improved quality of project end results • Reduced cost to deliver • Further cost savings due to more on-schedule project delivery
Requirements for compliance	To be compliant to the industry Standard, the PMBOK or PRINCE2 must be implemented to maturity level 2 **Process for compliance** • Implement the requirements of the PMBOK/PRINCE2 Standards to maturity level 2 and submit to a formal assessment by the IT Standards Council • If all requirements are met, the organisation will be deemed to have complied by the IT Standards Council.
Scope	The Project Management Standard shall be applicable to all the financial institutions and external (managed) service providers in the industry. • Organisations are required to implement either the PMBOK or PRINCE2 Standards to at least a maturity level 2.

Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council.

Key Elements of the Standards

PMBOK:

The PMBOK divides a project into 5 process groups that follow the Deming cycle:

- Initiating
- Planning
- Executing
- Monitoring & Controlling
- Closing

Simultaneously the project is also divided into nine knowledge areas as follows:

- Project Integration Management
- Project Scope Management
- Project Time Management
- Project Cost Management
- Project Quality Management
- Project Human Resource Management
- Project Communications Management
- Project Risk Management
- Project Procurement Management

Ref: http://www.pmi.org/PMBOK-Guide-and-Standards.aspx

PRINCE2:

PRINCE2 defines 40 separate activities and organized into seven processes:

- Starting up a project: In this process the project team is appointed, and a project brief is prepared. In addition, the overall approach to be taken is decided and the next stage of the project is planned.
- Initiating a project: This process builds on the work of the startup process, and the project brief is augmented to form a Business case. The approach taken to ensure quality on the project is agreed together with the overall approach to controlling the project itself. Project files are also created as well as an overall plan for the project.
- Directing a project: This process dictates how the project board should control the overall project. Directing a Project also dictates how the project board should authorize a stage plan, including any stage plan that replaces an existing stage plan due to slippage or other unforeseen circumstances. Also covered is the way in which the board can give ad hoc direction to a project and the way in which a project should be closed down.
- Controlling a stage: PRINCE2 suggests that projects should be broken down into stages and these sub-processes dictate how each individual stage should be controlled. Most fundamentally this includes the way in which work packages are authorized and received. It also specifies the way in which progress should be monitored and how the highlights of the progress should be reported to the project board. A means for capturing and assessing project issues is suggested together with

the way in which corrective action should be taken. It also lays down the method by which certain project issues should be escalated to the project board.

- Managing stage boundaries: This dictates what should be done towards the end of a stage. The next stage should be planned and the overall project plan, risk log and business case amended as necessary. The process also covers what should be done for a stage that has gone outside its tolerance levels. Finally, the process dictates how the end of the stage should be reported.
- Managing product delivery: This process has the purpose of controlling the link between the Project Manager and the Team Manager(s) by placing formal requirements on accepting, executing and delivering project work.
- Closing a project: This covers the things that should be done at the end of a project. The project should be formally de-commissioned, and resources freed up for allocation to other activities, follow on actions should be identified and the project itself be formally evaluated.

Ref: https://www.axelos.com/certifications/prince2

2.4 IT Operations

2.4.1 Business Continuity

Purpose	Framework to guide crisis management and ensure that critical services will always be available to customers and other stakeholders that must have access to those services
Justification	**Business Challenge** • Increased threat to Financial institutions – from political uncertainty, to terrorism, robbery to hackers/cyber threat, from civil unrest to insider fraud **How this Capability Addresses the business challenge** • An effective business continuity program enables Financial institution to not only reduce risk and improve recoverability, but also to provide a valuable service to the business, its customers, and its partners, all in alignment with the strategic business plan **Business Benefits** • Reduces business disruption threats as they are addressed before they occur which in turn improves business responsiveness • Reduces the impact of unplanned IT service downtime on business • Ensures optimum client delivery is maintained by providing support that strengthens management processes which allow the organisation to supply an agreed level of critical services/ products to the clients after disruption within a specified time frame • Promotes reputational management by reinforcing commitment to providing a premium level of services to stakeholders, even during adverse conditions • Saves cost by reducing the cost of internal and external audits which in turn improves Banking performance and reduce business disruption insurance premiums • Improves workforce relations and loyalty by focusing on workforce personal preparedness and workplace readiness

Standard	• Business Continuity Institute (BCI) Good Practice Guidelines (GPG): a management guide to implementing global best practice in Business Continuity Management • ISO 22301: A Business Continuity Management Standard that applies Business Continuity Planning to enterprises.
Version of the Standard to which Compliance is Required	• BCI GPG 2013 • ISO 22301:2012
Minimum Acceptable Maturity Level	• Level 2
Rationale for Selection	**BCI Good Practice Guidelines** • The BCI GPG is a holistic set of guidelines developed by the Business Continuity Institute which specifies six Professional Practices that cover all six phases of a Business Continuity Management Lifecycle: o Policy and Programme Management o Embedding BCM in the Organisation's Culture o Understanding the Organisation o Determining BCM Strategies o Developing and Implementing a BCM Response o Exercising, Maintenance and Review of BCM ISO22301 • Guidance on activities and deliverables applicable in establishing a continuity management process, as well as providing recommended good practice steps. It consists of 2 parts which details an auditable set of requirements o A Code of Practice which establishes processes, principles and terminology for Business Continuity Management o A Specification which details requirements for implementing, operating and improving a documented Business Continuity Management System and describes requirements that can be objectively and independently audited. The BCI GPG and the ISO 22301 both provide guidelines for Business Continuity Management
Benefits	• Assurance of business resilience and the capability to effectively respond to crisis situations. • Reduced exposure to risks by methodical risk identification • Reduced downtime
Requirements for compliance	BCI Good Practice Guidelines:

	To be compliant to the industry Standard the guidelines of the BCI GPG must be implemented within the organisation. ISO 22301: To be compliant, the organisation must implement a BCM System based on the requirements of Specification Section (Part 2) of the Standard **Process for compliance** BCI Good Practice Guidelines • Implement the requirements of the BCI GPG and submit to a formal assessment by the IT Standards Council • If all requirements are met, the organisation will be deemed to have complied by the IT Standards Council. ISO 22301 • Implement the controls specified in the specification section of the Standard • Request an assessment from an accredited ISO22301 auditor • Provide the results to the IT Standards Council as proof of compliance
Scope	This Standard shall be applicable to all licensed Payment Service Providers and National Microfinance Banks in the industry. • All organisations shall implement either the BCI GPG or the ISO 22301 guidelines. • ISO 22301 certification is mandatory for third party service providers in the industry.
Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council.

Key Elements of the Standards
BCI GPG: The Good Practice Guidelines specifies six Professional Practices which cover the six phases of BCM Lifecycle. These are grouped into 2 Management and 4 Technical Professional Practices • Management Professional Practices o Policy and Programme Management: The BCM Policy of an organisation provides the framework around which the BCM capability is designed and built. An effective BCM programme will involve the participation of various managerial, operational, administrative and technical disciplines that need to be coordinated throughout its life cycle o Embedding BCM in the Organisation's Culture: Developing a Business Continuity culture is vital to maintaining enthusiasm, readiness and effective response at all levels. It involves ▪ Assessing BCM Awareness and Training

        - Developing BCM within the Organisation's Culture
        - Monitoring Cultural Change
- Technical Professional Practices
    - Understanding the Organisation: understanding of the urgency with which activities and processes need to be resumed if they are disrupted and involves:
        - Business Impact Analysis
        - Risk Assessment
    - Determining BCM Strategies: determining and selecting BCM Strategies to be used to maintain the organisation's business activities and processes through an interruption. It includes:
        - Corporate Strategies
        - Activity Level Strategy
        - Resource Level Consolidation
    - Developing and Implementing a BCM Response: this aims to identify in advance, as far as possible, the actions that are necessary and the resources which are needed to enable the organisation to manage an interruption whatever its cause. It includes
        - Incident Management Plan
        - Business Continuity Plan
        - Business Unit Plans
    - Exercising, Maintenance and Review of BCM: A BCM capability cannot be considered reliable until it has been exercised, maintained and audited

Ref: www.the**bci**.org

ISO 22301

ISO 22301:2012 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. ISO 22301 is predicated on the established Plan-Do-Check-Act model of continuous improvement and covers the following:

- Planning the Business Continuity Management System (PLAN): The first step is to plan the BCMS, establishing and embedding it within the organisation.
- Implementing and Operating the BCMS (DO): This focuses on the actual implementation of the plans. This section includes several topics in Part 1.
- Monitoring and Reviewing the BCMS (CHECK): To ensure that the BCMS is continually monitored the Check stage covers internal audit and management review of the BCMS.
- Maintaining and Improving the BCMS (ACT): To ensure that the BCMS is both maintained and improved on an ongoing basis, this section looks at preventative and corrective action

Ref: http://www.iso.com

2.5 Information & Technology Security

2.5.1 Information Security and Payment Card Security

Purpose	Framework for ensuring that critical information assets are protected from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
Justification	**Business Challenge** • Increasing occurrence and popularity of data security breaches which results in fraud, the loss of personal information, and reputational damage **How this Capability Addresses the Business Challenge** • Prevents internal breach through training and awareness, communications, access control and back ground checks for individuals handling critical information assets • Increases visibility and comprehension of IT security issues, bringing preparedness to the workforce, which can help boost morale. **Business Benefits** • It provides assurance to customers, employees, trading partners and stakeholders that their personal and organisational information are secure and that there are policies and procedures in place to combat against possible breaches • Information security Standards helps embed the information security culture into the Bank as they cover the whole organisation, not just IT, and encompass people, processes and technology, so employees readily understand risks and embrace security controls as part of their everyday working practices
Standard	• ISO 27001/27002 is a globally recognized information security management Standard • Payment Card Industry Data Security Standard (PCI DSS) is a global Standard for information security defined by the PCI Security Standards Council which applies to all organisations that have cardholder data traversing their networks
Version of the Standard to which Compliance is Required	• ISO/IEC 27001:2013; ISO/IEC 27002:2013 • PCI-DSS Version 4.0
Acceptable Maturity Level	• Level 2
Rationale for Selection	**ISO 27001/27002** • ISO 27001 enables organisations establish and maintain an information security management system (ISMS). It focuses on how to implement, monitor, maintain, and continually improve the Information Security Management System

	• ISO 27002 provides established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organisation. It contains guidance on implementation of individual security controls, which may be selected and applied as part of an ISMS **PCI DSS** • This Standard is applicable to organisations that store, process and/or transmit credit and debit card data and aims to prevent card related fraud through increased controls around data. PCI DSS requirements are similar to some of the ISO 27001 certification requirements.
Benefits	• Increased customer confidence through assurance of higher level of data security • Increased protection against Banking losses and remediation costs that arise from security breaches
Requirements for compliance	PCI DSS: To be found compliant, the organisation must implement the specified controls within the agreed timelines and be ascertained by a Qualified Security Assessor (QSA) to have met the requirements for compliance. ISO 27001: An organisation must implement the necessary controls to meet the requirements of the Standard and be certified by an accredited certification body as such. **Process for compliance** PCI DSS • Implement required controls • Engage a QSA to conduct a formal assessment by the IT Standards Council • Provide the results to the IT Standards Council as proof of compliance ISO 27001 • Implement the requirements of the ISO 27001 Standard • Submit an application for assessment to an accredited certification body to conduct the formal assessment by the IT Standards Council. This is in 2 stages: o A review of the required documentation o A formal assessment by the IT Standards Council of the controls of the ISMS • Provide the results to the IT Standards Council as proof of compliance
Scope	This Standard shall be applicable to all Payment Service Providers and National Microfinance Banks in the industry.

	• PCI DSS compliance is mandatory for all organisations that store, process or transmit credit and debit card data. • The scope of compliance for ISO 27001/2 is: **E-Channels** o Cards: Visa card, Master card, Verve card etc. o Automated Teller Machine (ATM): mini Statement, withdrawal, inquiry, funds transfer, bills payment, airtime recharge o Point of Sale (POS): POS@Branch, LAN POS terminals, swipe loading key terminals, GPRS terminals, web monitoring interface o Web/Internet: bills payment, airtime top-up, funds transfer, balance enquiry, mini statement o Mobile: bills payment, airtime top-up, funds transfer, balance enquiry, comprehensive account statement **Data Center** o Event management process: data center events, event logs, changes which includes policies, principles, process activities, methods, triggers, inputs, and outputs o Incident management process: data center incidents such as outages, equipment loss and policies, principles, triggers, and techniques put in place for recovery o Problem management process: root cause analysis, comprehensive fixes, improvements, and knowledge library inputs for future problem resolution o Service operation practices: scope of operational support, analysis processes and functions o Request fulfillment process: end user and organisation requests for addition, removal or changes to infrastructure within the data center o Patching operating systems, database, applications and testing patches in a test or Quality Assurance (QA) environment prior to applying patches to production systems o Access management process: process for server, application, database, and physical access to the data center o Service Desk function: supports organisation with rules and responsibilities for service support to end users o Database performance management, administration and operation o Backup and recovery processes: routine backups, storage, recovery planning, and testing o Administrative planning and support: capacity planning, preventative maintenance and replacement **Information Assets in the Cyberspace**

	○ Information assets on the internet: websites, internet banking applications, mobile apps, information assets in the cloud and social media **Business Continuity (Optional)** ○ Business Impact Analysis (BIA): assessment and prioritization of all business functions and processes, identification of potential impact of business disruptions resulting from uncontrolled or non-specific events, Identification of legal and regulatory requirements for institution's business functions and processes, estimation of maximum allowable downtime, as well as the acceptable level of losses, associated with the business functions and processes, estimation of recovery time objectives, recovery point objectives, and recovery of the critical path ○ Risk Management: assessment and prioritization of all business functions and processes, prioritization of potential business disruptions based on severity, comparison between the existing Business Continuity Plan (BCP) and the policies/ procedures that should be implemented based on prioritized disruptions identified and their resulting impact on the institution and evaluating the business impact analysis assumptions using various threat scenarios. Reduction of risk to an acceptable level through the development, implementation, and maintenance of a written, enterprise-wide BCP ○ Risk monitoring and testing: incorporation of the business impact analysis and risk assessment into the BCP and testing program, development of an enterprise-wide testing program, assignment of roles and responsibilities for implementation of the testing program, completion of annual, tests of the BCP, evaluation of the testing program and the test results by senior management and the board, assessment of the testing program and test results by an independent party and revision of the BCP and testing program based upon changes in business operations, audit and examination recommendations, and test results • ISO 27001 certification is not mandatory.
Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council.

Key Elements of the Standards
PCI DSS: The PCI DSS Standard specifies twelve requirements for compliance across six control objectives as follows: • Build and Maintain a Secure Network ○ Install and maintain a firewall configuration to protect cardholder data ○ Do not use vendor-supplied defaults for system passwords and other security parameters

- Protect Cardholder Data
    - Protect stored cardholder data
    - Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
    - Use and regularly update anti-virus software on all systems commonly affected by malware
    - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
    - Restrict access to cardholder data by business need-to-know
    - Assign a unique ID to each person with computer access
    - Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
    - Track and monitor all access to network resources and cardholder data
    - Regularly test security systems and processes
- Maintain an Information Security Policy
    - Maintain a policy that addresses information security

PCI DSS: https://www.pcisecurityStandards.org/

ISO 27001 / 27002

ISO 27001 is based on the Plan-Do-Check-Act model and defines a set of information security management requirements as follows:

- Establish an ISMS
- Implement, operate, and maintain the ISMS
- Monitor, measure, audit, and review the ISMS
- Continually improve the ISMS

ISO 27002 contains guidance on implementation of individual security controls, which may be selected and applied as part of an ISMS. Controls are grouped into the following categories:

- Risk Assessment and Treatment
- Security Policy
- Organisation of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Access Control
- Information Systems Acquisition, Development, Maintenance

• Information Security Incident management • Business Continuity • Compliance ISO 27001: http://www.iso.org/

2.5.2 **Cyber Security**

Purpose	Cyber Security Standards helps Financial Institutions to defend the customer and organisational assets and counter cyber-attacks whilst coping with changing business requirements, speed to market pressures, expansion into emerging markets, business innovation requirements and budget constraints. They help Financial Institutions maintain their risk profile at an acceptable level.
Justification	**Business Challenge** • Cyber-crimes are increasing in scope and sophistication at a time when Financial Institutions are moving their key assets and systems to digital spheres and internet usage is growing significantly • Each year Financial Institutions lose billions of naira to fraud perpetuated through cyber-attack, sensitive personal information is exposed, and customer confidence is being eroded • Today's organized criminals are deploying a wide array of attack methods, such as e-mail scam and spam, ATM fraud, electronic banking frauds, man-in-the-middle attacks, falsifying customers information, card cloning, collusion with insiders, among many others • Damage to brand and reputation in the aftermath of an attack is perceived as a critical risk to Financial Institutions. **How this Capability Addresses these Challenges** • Complying with the Information Security Standards is one way to prove that your Financial Institution is taking cyber security threats seriously • Compliance enhances the Financial Institution's standing within the market and gives potential clients the assurance that your business has a managed, professional approach to protecting client data. This opens new opportunities & is especially attractive for banks – whose day to day business involves managing sensitive information. The volume and value of data produced and used in Finical Services institutions increasingly informs how the institutions operate and how successful they are. **Business Benefits** • Improves productivity and business growth as a result of the implementation of flexibly secure, integrity-assured, extensible services • Increases customer trust and loyalty by reliably safeguarding client and customer information and systems against threats and attacks • Increases shareholder value by reducing risk, costs and complexity
Standards	• ISO 27001/27002 • PCI DSS • ISO 27032

Version of the Standard to which Compliance is Required	• ISO/IEC 27001/21:2013; • PCI-DSS Version 4.0 • ISO/IEC 27032:2012
Minimum Acceptable Maturity Level	• Level 2
Rationale for Selection	**ISO 27001 /2** • ISO 27001 focuses on the establishment of a system of governance around cyber security within an organisation. • In ISO 27001/2 the organisations senior management takes full ownership of cyber security across the enterprise and the establishment of decision-making processes • It covers aspects such as human resources, physical assets, access control and governance, giving a holistic approach to cyber security • ISO 27002 provides best practices and recommendations on information security management, risks and controls. • All organisations are encouraged to assess their information security risks, then implement appropriate information security controls according to their business needs and risk appetite **PCI DSS** ▪ PCI-DSS gives a detailed list of requirements with regards to making the organisation's payment systems secure ▪ It identifies the need for monitoring and mitigating threats to the system and for incident management **ISO 27032** ▪ ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains. ▪ It covers the baseline security practices for stakeholders in the Cyberspace.
Benefits	• Organisations are equipped with a clear step by step approach to risk management with a detailed outline of the full risk management lifecycle; from identifying to mitigating cyber security risks • They give insight as to the cyber security roles that should be introduced as part of the ISMS • Organisations are better equipped and prepared to respond to cybercrime and other cyber security incidents

Requirements for compliance	• See Section 2.5.1 for requirement for ISO 27001/27002 and PCI-DSS • An organization cannot be certified in ISO 27032 but to be compliant, an organisation must develop and implement an end-to-end cybersecurity program to be verified by a ISO 27032 Cybersecurity manager to have met the requirements for compliance
Scope and Application	This Standard is applicable to all financial institutions and external (managed) service providers for the Financial Services industry
Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council

Key Elements of the Standards

ISO 27001 / 27002

ISO 27001 is based on the Plan-Do-Check-Act model and defines a set of information security management requirements as follows:

- Establish an ISMS
- Implement, operate, and maintain the ISMS
- Monitor, measure, audit, and review the ISMS
- Continually improve the ISMS

ISO 27002 contains guidance on implementation of individual security controls, which may be selected and applied as part of an ISMS. Controls are grouped into the following categories:

- Risk Assessment and Treatment
- Security Policy
- Organisation of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Access Control
- Information Systems Acquisition, Development, Maintenance
- Information Security Incident management
- Business Continuity
- Compliance

ISO 27001: http://www.iso.org/

PCI DSS:

The PCI DSS Standard specifies twelve requirements for compliance across six control objectives as follows:

- Build and Maintain a Secure Network
    - Install and maintain a firewall configuration to protect cardholder data

- Do not use vendor-supplied defaults for system passwords and other security parameters

- Protect Cardholder Data
  - Protect stored cardholder data
  - Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Use and regularly update anti-virus software on all systems commonly affected by malware
  - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Restrict access to cardholder data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes
- Maintain an Information Security Policy
  - Maintain a policy that addresses information security

PCI DSS: https://www.pcisecurityStandards.org/

ISO 27032

ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security,
- network security,
- internet security, and
- critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in Cybersecurity,
- guidance for addressing common Cybersecurity issues, and
- a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

ISO 27032: http://www.iso.org/

2.5.3 **Data Protection**

Purpose	Data Protection Standards helps Financial Institutions to defend the customer and organisational data ensuring data processing follows data privacy laws and best practices on data management
Justification	**Business Challenge** • No law exist to protect usage or processing of customer's data and also, data soverignty **How this Capability Addresses these Challenges** • Complying with the Data Protection Standards is a way to prove that Financial Institutions are taking data privacy seriously • Compliance enhances the Financial Institution's standing within the market and gives potential clients the assurance that your business has a managed, professional approach to protecting client data. This opens new opportunities & is especially attractive for banks – whose day to day business involves managing sensitive information. The volume and value of data produced and used in Finical Services institutions increasingly informs how the institutions operate and how successful they are. **Business Benefits** • Increases customer trust and loyalty by reliably safeguarding customer's information aligns to the data privacy law within and outside the country • Increases potential investors trust in data security within the financial eco-system
Standards	• Nigerian Data Protection Regulation(NDPR)
Version of the Standard to which Compliance is Required	• NDPR : 2019
Minimum Acceptable Maturity Level	Compliance with NDPR
Rationale for Selection	**NDPR** • NDPR is the current law guiding the data protection in Nigeria enacted by Section 6 (a,c) of the NITDA Act 2007 • Guidelines on data processing ,storage ,usage and security of customers are clearly defined
Benefits	• NDPR ensures that all personal information data of customers are adequately secured against theft, unauthorized usage or processing without customers consent • NDPR ensures data sovereignty within or outside the country and also, defined processes on usage outside the country

	• Organisations are aware of their responsibility in protecting customer data and avaliable sanctions on unauthorized usage
Requirements for compliance	To be compliant, an organisation must implement all NDPR guidelines
Scope and Application	This Standard is applicable to all financial institutions and external (managed) service providers for the Financial Services industry.
Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council

Key Elements of the Standards

NDPR

NDPR:2019 called Nigeria Data Protection Regulation defines security controls needed to be implemented towards the protection of Nigerian citizens within or outside the country either within the private or public sector.

It ensures the following;

- Safeguarding the rights of natural persons to data privacy
- Security controls in the processing of Personal Data
- Integrity of customers Personal Data
- Alignment to best practices on data security based on international standards

The controls ensures that all personal data aligns to the following;

- Collection and processing in accordance with specific, legitimate and lawful purpose consented to by the Data Subject
- Data stored is adequate, accurate and without prejudice to the dignity of human person
- Data storage is for a defined period
- Data stored is secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements
- Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject owes a duty of care to the said Data Subject
- Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject shall be accountable for his acts and omissions in respect of data processing, and in accordance with the principles contained in NDPR Regulation

NDPR: https://ndpr.nitda.gov.ng/

2.5.4 **Cloud Security**

Purpose	Cloud Security Standard helps Financial Institutions to defend the customer and organisational assets hosted in both private and public clouds like (Azure, AWS, GCP) by implementing necessary controls and stating roles and responsibilities for hosting asset in such environment for data protection. They help Financial Institutions maintain their risk profile at an acceptable level.
Justification	**Business Challenge** • Lack of standardization of processes for cloud operations and migration followed by majority of the popular Cloud Computing services – Microsoft Azure, Office 365, Amazon Web Services, Google Cloud Platform **How this Capability Addresses these Challenges** • Complying with the Information Security Standards is one way to prove that your Financial Institution is taking cloud security seriously • Compliance enhances the Financial Institution's standing within the market and gives potential clients the assurance that your business has a managed, professional approach to protecting client data. This opens new opportunities and is especially attractive for banks – whose day to day business involves managing sensitive information. The volume and value of data produced and used in Finical Services institutions increasingly informs how the institutions operate and how successful they are. **Business Benefits** • Wholistic risk management with an enhanced management of cloud service risks • Clearly defined roles and responsibility for both cloud service provider and cloud customer • Standardization of processes for cloud operations and migration. The standard is followed by majority of the popular Cloud Computing services – Microsoft Azure, Office 365, Amazon Web Services, Google Cloud Platform
Standards	• ISO 27017
Version of the Standard to which Compliance is Required	• ISO/IEC 27017:2015
Minimum Acceptable Maturity Level	• Level 2

Rationale for Selection	**ISO 27017** • ISO/IEC 27017:2015 provides security standard developed for cloud service providers and users to make a safer cloud-based environment and reducing the risk of a security breach • It provides security guidance on controls and practices that must be embedded in the usage of cloud infrastructure by providing; • Additional implementation guidance for relevant controls specified in ISO/IEC 27002; • Additional controls with implementation guidance that specifically relate to cloud services.
Benefits	• Organisations are better equipped on security control to be implemented where infrastructures are migrated to cloud environments • Clearly defined roles and responsibility for both cloud service provider and cloud customer
Requirements for compliance	To be compliant, an organisation must ensure the cloud provider of choice is ISO 27017 cerified and also, the organisation must have implemented adequate controls to secure data based on the security responsibility role to be ascertained by a Security Assessor to validate they have met the requirements for compliance
Scope and Application	This Standard is applicable to all financial institutions and external (managed) service providers for the Financial Services industry.
Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council

Key Elements of the Standards

ISO 27017

ISO/IEC 27017:2015 called code of practice for information security controls based on ISO/IEC 27002 for cloud services by adding additional security control for cloud services with the following key areas;

- Who is responsible for what between the cloud service provider and the cloud customer.
- The removal or return of assets at the end of a contract.
- Protection and separation of the customer's virtual environment.
- Virtual machine configuration.
- Administrative operations and procedures associated with the cloud environment.
- Cloud customer monitoring of activity.
- Virtual and cloud network environment alignment

It overs the baseline security practices for stakeholders in the Cyberspace. This International Standard provides;

- Scope
- Normative References
- Definitions and abbreviations

- Cloud sector-specific concept
- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

ISO 27017: http://www.iso.org/
http:// www.bsigroup.com

2.6 IT Innovation

2.6.1 Open Banking

Purpose	Provides a collaborative model in which banking data is shared through APIs between two or more unaffiliated parties to deliver enhanced capabilities to the marketplace.
Justification	**Business Challenge** • Difficulty with data access, thus, hindering the development of new products and business models by financial institutions. **How this capability addresses the business challenge** • Open banking stands to benefit end users as well as foster innovation and new areas of competition between banks and nonbanks, it will also usher in an entirely new financial services ecosystem, in which banks' roles may shift markedly. **Business Benefits** • Helps increase digital revenue • Improves overall customer engagement as it increases the appeal of a bank and enable them to meet the changing demands of existing customers as well as appeal to prospective customers • Enhances a financial services institution's service offerings
Standard	Open Banking Standard Version 3.1.2
Version of the Standard to which Compliance is required	Open Banking Standard Version 3.1.2
Minimum Acceptable Maturity Level	• Level 2
Rationale for Selection	• Provides a uniform model for ensuring collaboration and sharing of banking data
Benefits	• Improved customer experience • Sustainable service model for underserved markets • New revenue streams • Ability to access a far broader range of customer accounts
Requirements for Compliance	In order to be compliant to the industry Standard, the Open Banking standard version 3 must be implemented to maturity level 2.
Scope	This Standard shall be applicable to all PSPs and National MFBs
Exemption	An organisation may seek exemption from compliance by formal application supported by clearly articulated business justification to the IT Standards Council.

Key Elements of the Standard
Open Banking Standard Version 3.1.2 The latest version of the open banking standard, version 3.1.2 includes updates to the customer experience guidelines (CEGs) and operational guidelines (OGs). The Open Banking Standard is designed to assist account providers in meeting their PSD2 and RTS requirements as well as supporting their application for an exemption from the contingency mechanism. This market-enabling standard is built in an optional modular format to most effectively meet consumer and market needs. The standard covers all online payment accounts and includes the following core components: Read / Write API Specifications: These specifications consist of technical documentation, usage examples and swagger files. Security Profiles: These profiles have been developed together with the Open ID Foundation and cover third party on-boarding, re-direct and decoupled flows. Customer Experience Guidelines: These guidelines bring together regulatory requirements and extensive customer research to help third party providers deliver a great customer experience and avoid any unnecessary delay or friction as required under PSD2. Operational Guidelines: These guidelines support account providers implementing effective and high-performing dedicated interfaces while assisting them in fulfilling their regulatory obligations relating to performance and availability, design and testing, problem resolution, and management information. Open Banking Version 3.1.2: https://www.openbanking.org.uk

3 Considerations for IT Service Provider/Vendor Engagement

3.1 Considerations for Engaging IT Vendors and Service Providers

Most Financial Institutions in Nigeria rely on third-party vendors, service providers and other Banking institutions to provide system products, and services to their customers. Some rely on vendors to provide even operational functions.

The engagement of service providers in these capacities even with all the underling advantages presents various risks to the Financial Institution. Some of these risks are inherent to the solution being delivered while others are introduced by the involvement of the service provider. Due care needs to be exercised that these risks do not materialise, exposing the Financial Institutions to loss, regulatory action or even reputational damage.

The use of service providers does not relieve a Financial Institution's board of directors and executive management of their responsibility to ensure that service providers' activities are conducted securely and in compliance with the Financial Institution's Standards and in line with applicable regulations.

This section of the Blueprint provides guidelines for ensuring due care and diligence while engaging service providers:

1. **Policies and Procedures:** Develop policies on vendor/service provider engagement.

   Most Financial Institutions already have policies guiding interactions with contractors, vendors and service providers. This may already exist via the Financial Institution's business policies, or through the implementation of IT Standards like ITIL 4 and /or ISO 27001. CIOs are expected to conform to these policies where they exist and also ensure that they are aligned to the Financial Institution's IT Strategy. Where there is a misalignment or where the policy that exist does not address all the concerns for IT vendors, an addendum to the existing policy is recommended.

2. **Risk Assessment:** Conduct risk assessment to understand the implications of outsourcing a task or activity to vendors/service provider

   Financial institutions are encouraged to conduct a risk assessment of the business activity to be performed by the vendor and determine the implications of performing the activity in-house or having the activity performed by a service provider. The benefits, risks and cost implications which are a result of such an assessment are fundamental to deciding whether to perform an activity in-house, get a vendor to perform it in-house or outsource it to be performed from the service provider's location.

3. **Vendor Selection:** Exercise due diligence in the selection of vendors/service providers

   It is important that due diligence is exercised before a service provider is formally engaged.

   Activities recommended include: checking the service provider's background and reputation, policies, operations and internal controls, Financial performance, and business continuity /contingency plans (where applicable). Financial Institutions are advised to independently

validate and verify any certificates from certificate issuing authorises on the authenticity of the certificates presented by the vendors.

In particular, vendors providing specialised services are required to comply with the following:

Vendor Service Category	Applicable Standards
Payment Cards Processing or Payment Services Providers	▪ PCI Data Security Standard (PCI DSS) ▪ Payment Application Data Security Standard (PA-DSS) ▪ PIN Transaction Security (PTS) requirements ▪ The PCI Security Standards Council also maintains a list of Validated Payment Applications. For more information please visit https://www.pcisecurityStandards.org/ for more information
Data Center	▪ Telecommunications Industry Association's Telecommunications Infrastructure Standard for Data Center - TIA-942-B ▪ Information Security Management Systems — Requirements - ISO 27001
Cloud	▪ Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – ISO 27018 ▪ Information Security Management Systems — Requirements - ISO 27001

The depth and formality of the due diligence activities performed depends on the criticality of the business activity to be performed by the vendor.

4. **Contracting:** Implement thorough and rigorous contracting procedures.

   The contract with the vendor/service provider must be drawn up in conjunction with and reviewed by the Financial Institution's legal department. All contracts should contain at the minimum:

   i. Scope of services to be provided
   ii. Service performance requirements
   iii. Division and agreement of responsibilities
   iv. Contact points, communication and reporting frequency and content
   v. Training of Financial institution employees
   vi. Contract review and dispute resolution processes
   vii. Price structure and payment terms
   viii. Compliance with applicable laws, regulations, regulatory guidance and Standards
   ix. Intellectual property rights and copyright

x. Right to audit: Contracts should contain the right of the Financial Institution or its representatives to audit the service provider and/or to have access to audit reports

xi. Liability limitations

xii. The ability to subcontract services

xiii. Termination rights of each party

xiv. Obligations at termination and beyond

5. **Monitoring and Enforcement:** Enforce continuous oversight and monitoring of service providers.

   It is recommended that the contract should define measurable performance standards for the services or products being provided. Financial Institutions are encouraged to monitor vendors/service providers for compliance with contracts and service level agreements. Financial Institutions are encouraged to validate business continuity and contingency plans for vendors /service providers who support critical business functions or provide mission critical activities

Financial Institutions are encouraged to establish and maintain effective vendor/service provider management programs to derive full benefits from engaging service providers while mitigating inherent risks.

4 Frequently Asked Questions (FAQ)

The table below is an excerpt of some of the frequently asked questions on IT Standards asked and responses to them:

S/N	Feedback from the Banks	Response
1	Will CBN certify Financial Institutions that are compliant with respect to the IT Standards?	The CBN through the IT Standards Council will not certify banks. Certification will be left for the Certificate Authorities
2	Who will determine the acceptability of local variations of Standards and how would this be achieved?	IT Standards Review Committee is responsible for the review and evaluation of IT Standards on an annual basis to determine their continued relevance to the local industry. Where these Standards are found to require a local context, this will be recommended to the IT Standards Council after a thorough review by the committee.
3	Will Implementation Guidelines suffice (in the interim) for Banks towards full compliance?	Implementation guidelines from certification authorities will suffice. However, a minimum of maturity 2 is required for all PSPs and National MFBs.
4	Can a phased maturity plan be adopted by PSPs and National MFBs to attain maturity level 2	Phased maturity plans can be adopted by PSPs and National MFBs. However, both PSPs and National MFBs will be expected to meet the minimum acceptable maturity level on or before the deadline for such Standards.
5	How many Standards per capability area are required by the PSPs and National MFBs to implement?	PSPs and National MFBs are required to implement as agreed in the roadmap per area of IT concern. PSPs and National MFBs that want to implement more than one Standard are welcomed.
6	Who would be responsible for ensuring compliance for services/ IT Standards provided by the Service provider?	All organisations that would be responsible for providing services to the industry will be subject to the industry IT Standards. However, the existence of service providers does not preclude PSPs and National MFBs from implementing the IT Standards.
7	Can the PSPs and National MFBs extend the scope of new and already implemented Standards?	PSPs and National MFBs can extend the current Standards as long as the minimum features / requirements of the Standards defined for the Industry are met
8	Are PSPs and National MFBs with foreign affiliation required to adopt the IT Standards?	Yes. Standards defined for the local industry are expected to be adopted by every PSPs and National MFBs irrespective of affiliation or parentage.
9	Will self-audit/assessment by a PSPs and National MFBs internal formal assessment by the IT Standards Council sufficient?	Internal audits / checks may be performed to ensure PSPs and National MFBs own compliance. However only reports from the Compliance Management Committee and Independent Assessors will be used for compliance purposes by the IT Standards Council.

S/N	Feedback from the Banks	Response
10	Will there be exemptions for some PSPs and National MFBs with regards to adopted IT Standards?	There will no exemptions. All PSPs and National MFBs will be required to implement all agreed IT Standards
11	How would new, excluded or obsolete IT Standards e.g. risk management, PCI-DSS etc. be reviewed?	All new/ additional Standards will be reviewed during the annual IT Standards review and recommendations made to the IT Standards Council
13	Will the implementation of IFRS taxonomy as part of the mandatory migration to IFRS based reporting suffice for XBRL compliance?	For PSPs and National MFBs reporting, implementation of the IFRS taxonomy suffices for XBRL compliance. However, it does not cater to other forms of business information reporting

5 Appendix

5.1 IT Trends and the Implications for the Nigerian Financial Services Industry

Globally the Financial Services industry has undergone significant changes. Technology has transformed the industry in countless ways over the past 30 years.

The emergence of digital technology trends such as:

- Cloud Computing
- Social Media
- Big Data
- Technology outsourcing
- Mobility
- Artificial intelligence
- Internet of Things
- Distributed Ledgers
- Intelligent Process Automation

drive innovations in operations and customer service in the Financial institutions. These trends are touted to solving the challenges of the 21st Century Financial Institution; handling the increasing complexities of business while satisfying the customers need for convenience and to abide by increasingly complex regulatory rules.

Successful Financial Services institutions are customer focused. The adoption of digital and mobile technology by consumers has raised the expectations to an always available, real-time, on-line customer experience across all service channels. It's been proven that these trends can help Financial institutions meet customer expectations.

IT Standards covering these trends are still evolving .What we have are guidelines localized in different countries where they exist. Guidelines for adoption of these trends for the Financial Services industry in Nigeria have not been included in this version of the Blueprint but are expected to be included in future revisions of this blueprint after proper industry engagement.

In this section we explore the highlighted trends, as well as the risks, benefits and potential impact on the Financial Services Industry in Nigeria.

5.1.1 Cloud Computing

Cloud computing offers a value proposition that is different from traditional enterprise IT environments. It provides a way of exploiting virtualization and aggregate computing resources and thereby offer economies of scale that would otherwise be unavailable. With minimal upfront investment, Cloud computing enables global reach of services and information through an elastic utility computing environment that supports on-demand scalability. It also offers pre-built solutions

and services, backed by the skills necessary to run and maintain them, potentially lowering risk and removing the need for the organisation to retain a group of scarce highly skilled staff.

Implications (Positive) of Adopting Cloud Computing

- Cost Efficiency: Cloud computing eliminates the investment cost on standalone servers and respective software. The organisation can save on license costs and the time required to setting up these servers. Also, the Cloud infrastructure takes up the maintenance and software updates required on these servers
- Convenience and Continuous Availability: The services offered by a public Cloud are available over the internet and can be accessed from anywhere. Users across different time zones and in geographic locations can easily access services. The Cloud also guarantees continuous availability of these services
- Backup and Recovery: Cloud computing simplifies the process data backup and recovery as the data resides in Cloud and not on a single physical device. Different service providers offer reliable and flexible backup/recovery solutions
- Faster deployment and simple Integration: Cloud based system can be easily setup in a very short period of time. The addition of new instances can be performed very quickly. In a Cloud environment, software can easily be integrated. Hence, minimum effort is required to customize and integrate the applications. The addition of new instances can be performed very quickly. In a Cloud environment, software can easily be integrated. Hence, minimum effort is required to customize and integrate the applications
- Storage capacity: The Cloud offers almost unlimited storage capacity. Thus, the worry of running out of space or upgrading hardware have been addressed
- Environmentally friendly: The Cloud infrastructure requires fewer resources than the typical IT infrastructure. Only the resources that are truly required are consumed by the system

Risks in Adopting of Cloud Computing

- Security and privacy: By outsourcing the IT infrastructure, the Financial Institutions gives away data that might be sensitive and confidential. The organisation has to rely on the provider to maintain the security of their data. Data security is such a vital issue that all possible alternatives must be explored before taking the final call to implement Cloud computing, as the existence of the organisation could be in danger if data is leaked
- Dependency: Dependency is one of the major drawbacks of Cloud computing. This results in “vendor-lock-in" as it difficult to migrate from one Cloud vendor to another because of the huge data migration effort required.

- Vulnerability: In Cloud computing, since every component is available on the Internet, the risk of the entire environment being highly vulnerable to hackers and unwanted users is always there
- Downtime: Outage and downtime are two of the most important aspects that even the best service provider of Cloud computing can't absolutely guarantee. Also, you must keep in mind that the whole setup is Internet based. Thus, any downtime on the Internet side will lead to a connectivity issue
- Regulation: The rules governing the cloud vary from country to country. Some country data protection laws impose constraints on where data is kept, limiting take-up. Currently, in Nigeria, there are no guidelines or regulation regarding hosting organisational information in the cloud.
- A gradual implementation approach is suggested for successful transition to cloud. This follows a slow migration process that steadily increases the number of processes or functions being hosted by the cloud. This migration approach is dependent on the ability for an objective assessment of the readiness of each individual service, and the components thereof, to be migrated to the cloud. The risk of moving highly confidential Financial information to the public cloud can be enormous if not properly controlled

5.1.2 **Social Media**

Internet penetration in Nigeria currently stands at about 33%[1] with over 56 million internet users. The impact of the Internet and Social Media on the Nigerian economy is significant and has grown rapidly over the years. Social networking and social media technologies are widely believed to offer business and governmental organisations, a powerful means to deliver deliver superior customer experience by improving their communications, processes and, ultimately, performance. The Financial industry is fully aware and is taking measures to tap into the benefits of social media.

Today, the Financial industry is using social media in a variety of ways including advertising and marketing, soliciting feedback from the public, engaging with existing and potential customers, facilitating applications for new accounts and providing incentives. The continuous growth and opportunities in social media, generates growth in social media risks for Financial institutions.

Implications (Positive) of Adopting Social Media

- Improves search engine optimization rankings and brand recognition: Having social media pages makes the organisation look legitimate and trustworthy to search engines. The more an organisation engages in social media conversation, the more likely the organisation will show up on the top in search engines. This would in turn lead to increased brand and product awareness among prospective customers

- Builds customer loyalty: An organisation that engages customers on social media platforms by sharing news about promotions or new hires, new products or special incentives, community involvement, pictures etc. would enjoy higher loyalty from their customers awareness among prospective customers
- Decreases marketing cost: Writing a tweet, Facebook update, or any other posts on the various social media channels is free. Placing an advert on social media or promoting a post is cheaper than sending out thousands of mailers or producing a TV commercial.
- Provides better customer service and insights: Social media is extremely beneficial for fielding customer comments, concerns, and questions. Customers can easily and conveniently communicate directly with the Financial Institution and can quickly be answered in a public format that lets other customers/members and prospects see your responsiveness.

Risks in Adopting Social Media

- Brand strategy: Wrong online brand strategy could put the organisation at a viral social disadvantage and may even damage its reputation, i.e., when you make a mistake offline, a few will know but when you make a mistake in front of hundreds or thousands online audience, most of them will know
- Clear understanding of Social Media: In order to get social media's full effect, the organisation need to understand how it works, when and how to use it and which channels to focus on depending on and the end goal of using social media
- Return on Investment (RoI): It is difficult to quantify the return on investment and the value of the different channels
- Brand reputation: If the customer feels they haven't been treated appropriately, they have powerful tools at their disposal (Facebook, Twitter, etc.) to express their side of the story and negatively impact a brand reputation

NITDA released Framework and Guidelines for the Use of Social Media Platforms in Public Institutions in January 2019. Some of the guidelines introduced include:

All Public Institutions, in using social media, shall:

- Obey relevant laws, policies and regulations related to the use of ICT in the cyberspace;
- Use official email(s) for social media account;
- Establish an account handover processes for social media handlers who leave the organisation;
- Maintain high standard of professional conduct and behavior on social media;
- Establish authority to vet information being posted on social media;

- Establish protocols in relation to who is authorised to respond to inquiries received via social media;
- Ensure only authorised spokespeople or duly delegated officials provide comment to the media on government-related issues.

Government official, in using social media, shall:

- Not use personal social media accounts for official engagement;
- Not publish personal opinions on official social media accounts;
- Respect copyright laws;
- Ensure postings or comments are factual, ethical, respectful, apolitical, impartial and professional;
- Require permission from the authority before posting anything on the social media;
- Represent the PI professionally and be sure that what is published is consistent with relevant policies, standards, executive orders and circulars related to the mandates of the organisation;
- Not disclose information, nor make commitments or engage in activities on behalf of the PI on social media unless authorised to do so;
- Not engage in harassment, bullying, illegal or otherwise inappropriate activity while using official social media account;
- Not divulge confidential information or post what represents "official view" unless authorised to do so; and
- Observe and respect the code of conduct for public servants and public service rules when using private social media account in a private capacity on public discussion.

5.1.3 **Technology Outsourcing**

Outsourcing involves the provisioning and blending of business and IT services from a mix of internal and external providers. Effective management of the service provider is important to ensure that service levels are met, and that delivery is driven by continuous improvement of its processes

In recent years, Financial institutions have witnessed a steady acceleration and expansion in Technology outsourcing. It represents an opportunity for Financial Institutions to refocus on their core competences in order to add more value, while getting best-of-breed services for daily operations from a professional specialist. Outsourcing is a cornerstone to maximizing returns for shareholders, while enhancing product developments and improving service effectiveness.

The Financial industry must re-evaluate their strategy for sourcing technology because the market has changed. Trying to do everything is now equivalent to doing nothing. In an environment of growing

size and complexity, increased competition and the current need to recover balance sheets after the recent crisis, technology outsourcing is the answer.

Implications (Positive) of Adopting Technology Outsourcing

- Accelerate migration to new technology: Outsourcing of IT processes increases productivity and quality by reducing downtime
- Reduces risk: Every business investment carries a certain amount of risk. Markets, competition, government regulations, and technologies all change very quickly. Outsourcing providers assume and manage much of these risks for the organisation with specific industry knowledge, especially security and compliance issues
- Lower infrastructure investments by reducing infrastructure expenses, call centers and IT Service desk cost.
- Reduce labour costs: Hiring and training an IT staff can be very expensive, and temporary employees do not always live up to expectations. Outsourcing enables the business to focus human resources where they are mostly needed.
- Increases efficiency and competitiveness by reducing research, development, and implementation costs which are ultimately passed down to the customers.
- Businesses have limited technical, Banking and human resources. Outsourcing will help the organisation stay focused on core business and not get distracted by complex IT decisions.

Risks in Adopting Technology Outsourcing

- Hidden costs: Although outsourcing is usually cost-effective, the hidden charges involved in signing a contract especially those across international boundaries may pose a serious threat.
- Lack of customer focus: An outsourced vendor may be catering to the expertise-needs of multiple organisations at a time. In such situations, vendors may lack complete focus of the organisation's tasks.
- Synchronizing the deliverables: Some of the common problem that can be associated with IT outsourcing includes stretched delivery time frames, sub-Standard quality output and inappropriate categorization of responsibilities. At times it is easier to regulate these factors inside an organisation rather than with an outsourced partner.
- Loss of managerial control: When another company is assigned the task to perform the function of an entire department or single task, the management and control of that function is being handed over to another company. Although a contract exists, the managerial control will belong to another company. The outsourcing company will not be driven by the same Standards and mission that drives the business. They will be driven to make a profit from the services that they are providing to the organisation.

- Threat to security and confidentiality: The life-blood of any business is the information that keeps it running. If confidential information is transmitted to the outsourcing company, there is a risk of it been compromised. If the outsourced involves sharing proprietary company data or knowledge, this must be taken into account. There is the need to evaluate the vendor critically to ensure the proprietary data is well protected from unauthorized access. Also, the penalty for a data breach should be clearly communicated.

5.1.4 **Big Data**

Big data is characterized by the tremendous volumes, varieties and velocities of data that are generated by a wide array of sources, customers, partners and regulators. Financial Institutions that can harness big data, in the form of transactions, real-time market feeds, customer-service records, correspondence and social media posts, can derive more insight about their business than ever before and build competitive advantage. Successfully harnessing big data can help Financial Institutions achieve three critical objectives for transformation:

- Create a customer-focused enterprise
- Optimize enterprise risk management
- Increase flexibility and streamline operations

Big data is touted to empower Financial institutions understand and profile its customers in much greater detail than before.

Big data capabilities provide Financial Institutions the ability to understand their clients at a more granular level, anticipate their needs and quickly deliver targeted personalized offers. This improves customer profitability, satisfaction and retention. Being able to anticipate your customer needs and resolve them before they become problems allows Financial Institutions to deliver timely, concise and actionable insight to contact center agents which can lead to increased sales, improved customer satisfaction and a reduction in operating costs.

There are a number of things currently holding back the Financial sector, one of which is 'Data' which is disparate and locked away in a range of systems. Not embracing this information, and the opportunities it presents, denies access to a market that could save Financial Institutions millions of Naira annually.

Implications (Positive) of Big Data Analytics

- Service improvement: Big data analytics improves services dramatically by monitoring customer's behavior, interaction, sentiments data across call centers, blogs, forums, and social media platforms into deeper analytics. This in turn would lead to higher conversion rate and extra revenue.

- Improved sales: Better sales insights, which could lead to additional revenue. Big data analytics tell exactly how the sales are doing and when the product is not doing extremely well, it can take action to prevent missing out or losing revenue.
- Keep up with customer trends: Big data provides insight into competitive offerings, promotions or customer spending pattern which provides valuable information regarding customer trends.

Risks in Adopting Big Data

- Data quality: The greatest impact of Big Data is on data quality. To ensure the highest form of data quality and integrity, data validity, accuracy, timeliness, reasonableness, completeness must be clearly defined, measured, recorded, and made available to end users. If data is mapped or cleansed, care must be taken not to lose the original values.
- Privacy and security: The potential for abuse of data is significant as data migrate from one system to another.
- Executive buy-in: It is very difficult to get executive buy in to approve investment in big data and its related investments.

5.1.5 **Mobility**

Mobility is reshaping Banking customer engagement in a dramatic manner. Due to mobile's ubiquity and ease of use, consumers are tethered to their mobile devices to an extent unmatched by any other technology in the past. And for many, mobile is increasingly becoming the primary method of interaction with their Banking providers.

Emerging technology forces in the Financial Services industry are already impacting business. The convergence of these forces does present challenges; however, it also provides a window of opportunity for Financial institutions to elevate business performance and gain a competitive advantage.

Mobility fosters Financial inclusion by helping underserved consumer's access safe, convenient, and affordable Banking by encouraging more Financial -services providers to offer mobile-account capabilities for the underserved.

Mobility offers value, utility, and convenience on bill payment by reducing cost and time spent paying bills and offering consumers more control over when and how they pay. Several products offer a virtual-check feature through mobile websites and apps as a more convenient and less expensive alternative to money orders.

Implications (Positive) of Adopting Mobility

- Improves banking: The advent of banking mobile apps has transformed the face of banking the way traditional internet banking could not. This is because the device required for mobile banking is more portable and, in most cases, cheaper than a Personal Computer—the device for traditional internet banking.
- Reduces total cost incurred by customer: The Banking industries offer mobile Banking at prices lower than what the customer would have to incur if he/she had to be involved in normal banking transactions where visiting the organisation would be necessary.
- Two-way benefits: Mobility does not only benefit the customers but also the Banking organisation. It is a cost-effective solution for Banking industries, as they no longer have to spend on tele-banking. Moreover, it helps the Banking industry understand the way customers make monetary transactions, and hence they can improvise on means to better their customer care services. They can also identify their target customers better and promote services and products such as different types of loans and credit cards to different section of audience.
- Reduces Fraudulent Transactions: Most Financial institutions now offer security codes to their mobile customers in order to ensure added security while using apps for making transactions. Contrary to the popular belief that mobile banking apps are not secure, these types of software are now offering enhanced security features to their customers. The possibility of fraud is reduced since the customers using mobile banking apps are alerted via Short Message Service (SMS) every time an activity is conducted in their accounts. As soon as money is deposited or withdrawn from bank accounts through activities such as fund transfer, check deposit, or cash withdrawal, the customer will receive an SMS alert on his/her mobile device irrespective of whether the smartphone is connected to the internet or not**.**

Risks in Adopting Mobility

- Security: Mobile users are especially susceptible to scam. Most scam involve fraudulent text messages sent out to unsuspecting mobile banking users to provide their bank account details for a required service. Many customers fall for this trick and have given unauthorized persons access to their funds.

5.1.6 **Artificial Intelligence**

Artificial Intelligence emphasises the creation of intelligent machines that work and react like humans. Analysts estimate that AI will save the financial industry more than $1 trillion by 2030.

Increased AI usage can be used to create more personalised services to ensure customer satisfaction, improve efficiency and maintain customer loyalty. In addition to this, AI has the potential to help financial institutions become more efficient in the process of detecting fraud and money laundering.

AI enables faster, and more personalised services facilitated through automated machines and software.

Implications (Positive) of Adopting Artificial Intelligence

- Fraud Prevention: AI systems, through machine learning, can monitor and detect irregular and anomalous behaviours in transactions and purchases and flag them to be checked by experts. The advantage here is that AI can go through these transactions faster than any group of humans could ever do and learn on-the-go to help reduce the occurrence of "false-positives".
- Better Trading Information: AI systems can trawl through large amounts of customer-related data faster and more efficiently. This enables financial service providers to better understand behavior traits of customers and prospects, enabling them to quickly predict and determine trends and outcomes. This helps them stay ahead of the curve and make faster trading and investment decisions.
- Compliance to Regulations and Rules: AI systems can be used to develop a framework to help ensure that regulatory requirements and rules are met and followed. Through machine learning, these systems can be programmed with regulations and rules so as to serve as a watchdog to help spot transactions that fail to adhere to set regulatory practices and procedures. This helps ensure real-time automated transaction monitoring to ensure proper compliance with established rules and regulations.
- Risk Assessment and Minimisation: AI can be useful for reviewing large data caches and financial histories of companies and the market at large. This makes it useful in assessing and pointing out business and investment risks which can then be addressed and resolved. AI can also be programmed to make investment decisions autonomously using processed information or with human oversight.
- Determine Credit Worthiness: AI systems can help financial institutions determine which customers or businesses are safe to provide loans to and which are not. Through specific algorithms and processes, these AI systems can help banks determine which customers they should grant loans to and which customers to not.

Risks in Adopting Artificial Intelligence

- Cost of Operation: Production and maintenance of AI requires huge costs as they are very complex machines. AI also consists of advanced software programs which require regular update to meet the needs of the changing environment. In the case of critical failures, the procedure to reinstate the system may require enormous time and cost.
- Bad Calls: Although AI can learn and improve, it can't make judgement calls. Humans can take individual circumstances and judgement calls into account when making decisions, something

that AI might never be able to do. Replacing adaptive human behavior with AI may cause irrational behavior with ecosystems of humans and things.

5.1.7 Internet of Things

With the rapid digitisation and mobilisation in the financial services industry, it is important to explore the possibility of IoT in finance to leverage data and to minimise the risks that are endemic to this sector.

Implications (Positive) of Adopting Internet of Things

- Optimized Capacity Management: Banks and financial institutions can analyse the usage of ATM points and offices in specific areas and use this information to increase / decrease the installation of ATMs depending on usage volumes. Along with ATMs, banks can also use IoT data in bringing on-demand services closer to customers.
- Payment Transaction Security: Financial services can use IoT in predicting fraud in debit / credit card transactions. When a customer swipes his / her card, by verifying account holders mobile / device location and the transaction location, the bank can confidently approve or decline the transaction accordingly.
- Personalized Offerings and Rewards: IoT-enabled data analytics will make it easier to increase customer engagement and loyalty by offering customers loans as well as investment options based on specific characteristics such as the value of their assets, their spending habit, etc. IoT-based intelligence can be sued to entice customers by rewarding relevant redeemable options based on demographics and shopping options.
- Simplified Debt Collection: Monitoring the operations and supply chain activities of debtor businesses using IoT sensors and networks can help FSIs to determine their readiness to pay without involving excessive overhead costs.

Risks in Adopting Internet of Things

- Privacy: All transaction data, including the information sent through smart devices and smart watches, will be available to financial institutions. Along with data, these institutions might also have access to customer location, which may lead to a breach of privacy. Adhering to privacy standards while making good use of information is a great area of concern.
- Data Security Risk: Financial Institutions collect a lot of information from customers through various channels. Any data breach could lead to severe repercussions for banks. Data infringement and data hacking may cause massive damage to customers and fracture the relationship with their banks.

- No Uniform Standards: IoT software is developed by various companies, and programmes are not all mutually compatible. Some devices may simply be incapable of communicating with specific apps or programmes, which can be a problem for the users.
- Complex Networks: The larger the network, the more difficult it is to maintain, and IoT is no exception. Maintenance is tricky, as an ill-conceived solution could potentially cause a plethora of new issues. It is important to carefully screen both manufacturers and asset managers, as those who lack IoT experience can unleash catastrophe across a network.

5.1.8 Distributed Ledgers

Distributed ledger Technology (DLT) has the potential to transform well-established financial institutions and bring lower costs, faster execution of transactions, improved transparency, auditability of operations, and other benefits.

Implications (Positive) of Adopting Distributed Ledger Technology

- Instant Settlements: With DLT, settlements become more user-optimised, which will save a significant amount of time and money, for both parties involved. This technology will remove the need for a lot of middle office and back office staff at banks, as transactions settle immediately.
- Reduced Counterparty Risks: When transactions are settled near instantly, it will remove a significant part of the risk that the counterparty cannot meet its obligations, which could be a substantial expense for banks.
- Improved Capital Optimisation: One of the main features of DLT is that it removes the need for a trusted intermediary and makes peer-to-peer transactions possible. DLT offers better capital optimization, due to a significant reduction in operational costs for banks.
- Reduced Error Handling and Reconciliation: A key feature of DLT is that any data recorded is immutable. Any data that is recorded on a blockchain can be tracked in real-time, leaving a very detailed audit trail. As such, it eliminates error handling and reconciliation.
- Increased Transparency: Increased Transparency among financial institutions and as such improved regulatory reporting and monitoring by central banks, if the regulators also have access to the DLT.

Risks in Adopting Distributed Ledger Technology

- Lack of Standards and Regulation: One of the primary DLT security issues is the lack of regulation or standards. The lack of standard protocols mean DLT developers cannot easily benefit from the mistakes of others, hence no uniformity.

5.1.9 Intelligent Process Automation (IPA)

Intelligent Process Automation (IPA) has the potential to transform just about every area of the finance function. In particular, IPA will enable finance professionals to make the critical shift from transactional to strategic.

Implications (Positive) of Intelligent Process Automation

- Improves Functional Operations: IPA often automates repetitive manual processes, allowing organisations to redirect staff to other more strategic and innovative work that requires human judgement and discretion. This frees up the organisational capacity of the financial institution.
- Easy Account Reconciliations: IPA is capable of not only recognizing patterns, but also identifying the issue at hand and correcting it. In many cases, this can be done without the need for any human input.
- Reduced Operating Cost: The cost of using a software robot has been estimated to be 1/9 of the cost of on-shore FTE and 1/3 of the cost of an off-shore FTE. As the technology matures these differentials will only increase.
- Improved Insight: IPA provides insight into the operations of FSIs from the improved analytics that can be derived from digitized business processes. These analytics can be made available in real-time or on a periodic basis, giving senior stakeholder better quality insights with which to view operational performance and adapt their business as required.

Risks in Adopting Intelligent Process Automation

- Maintenance and Operations: Although Intelligent Processes are configured based on defined business requirements, broader architecture and system changes can severely affect the expected performance. Modified data field mappings, vendor upgrades, system integrations, etc., require attention to preserve the original intentions of the Intelligent Process and manage the perceived brittleness of the application and IPA dependencies.
- Cybersecurity and Resiliency: As robotics and intelligent processes become mainstream, these new entrants to the IT environment represent additional vectors for compromise. Platform security vulnerabilities, privacy implications and denial of service may yield ramifications that impact the IPA integrity, reliability and downstream business processes.

END OF DOCUMENT