Nigeria Banking Industry
IT Standards Blueprint

Version 2.1

April 2015

PREAMBLE

This IT Standards Blueprint document presents the framework for the adoption of Information Technology (IT) Standards for the Nigerian Banking Industry.

This document encourages Banking 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 Banking 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 Banks 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 Unit, the IT Standards Council, and Nigerian Banking 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 Unit

Table of Contents

PREAMBLE **2**

LIST OF FIGURES AND TABLES **4**

ABBREVIATIONS **5**

1 INTRODUCTION **6**
1.1 Background 6
1.2 Revision of the IT Standards Blueprint 7
1.2.1 Summary of Changes to the IT Standards Blueprint 7
1.3 Objectives and Purpose of Document 9
1.4 Definition of Standard 9
1.5 Overview and Summary IT Standards for the Nigerian Banking Industry 9
1.6 Target Maturity Levels 12

2 IT STANDARDS BLUEPRINT **15**
2.1 Strategic IT Alignment 16
2.2 IT Governance 19
2.3 Architecture and Information Management 23
2.4 Solutions Delivery 33
2.5 Service Management and Operations 41
2.6 Information & Technology Security 60
2.6.1 Information Security and Payment Card Security 60
2.6.2 Cyber Security 66
2.7 Workforce & Resource Management 69

3 RE-PRIORITISED INDUSTRY IT STANDARDS **73**
3.1 Re-prioritised IT Standards 73
3.2 IT Standards Adoption Roadmap 75

4 CONSIDERATIONS FOR IT SERVICE PROVIDER/VENDOR ENGAGEMENT **76**
4.1 Considerations for Engaging IT Vendors and Service Providers 76

5 FREQUENTLY ASKED QUESTIONS (FAQ) **80**

6 APPENDIX **82**
6.1 IT Trends and the Implications for the Nigerian Banking Industry 82
6.1.1 Cloud Computing 82
6.1.2 Social Media 85
6.1.3 Technology Outsourcing 86
6.1.4 Big Data 88
6.1.5 Mobility 89

List of Figures and Tables

Figure 1 - IT Standards Prioritization.....73
Figure 2: IT Standards Implementtaion and Adoption Timeline 75

Table 1: Summary of changes to the Blueprint.....9
Table 2: IT Capability Areas 10
Table 3: IT Capability Areas and IT Standards.....11
Table 4: Definition of Maturity Levels.....13
Table 5: Description of Level 3 Maturity.....14

Abbreviations

ITCMM	IT Capability and Maturity Model
ITIL	IT Infrastructure Library
COBIT	Control Objectives for Information and Technology
ISACA	Information Systems Audit and Control Association
XBRL	eXtensible Business Reporting Language
TOGAF	The Open Group Architecture Framework
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
OHSAS	Occupational Health & Safety Advisory Services
BCI	Business Continuity Institute
PCI DSS	Payment Card Industry Data Security Standard
SFIA	Skills Framework for the Information Age

1 INTRODUCTION

1.1 Background

Globally, Banking Institutions depend on Information Technology (IT) to help them achieve their vision, and strategy. IT has transformed the ways Banking 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 Banking Industry in Nigeria.

Over the past 20 (twenty) years, there has been a consistent increase in IT investments by Nigerian Banking 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 organizational 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

To address this gap 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 Banking Institutions.

The IT Standards Blueprint was developed in 2010 and published in 2014, after undergoing a minor update in 2013.

It has been 5 years since the Blueprint was developed. Within this period a number of changes have occurred within the industry and the IT Standards space necessitating the detailed review of the Blueprint. Some of these changes include:

- Some Standards in the original Blueprint are outdated, withdrawn and superseded by new Standards
- Technology trends such as cloud computing, social media, mobility, managed services now have significant impact on the operation and products of Banking institutions

- Cybercrime is increasing in scope and sophistication
- Feedback from the industry revealed that a number of banks face a number of challenges in implementing the Standards Blueprint. Most banks experience difficulty in obtaining senior executive buy-in for the implementation of the Standards recommended in the Blueprint

Based on the reasons highlighted above, the IT Standards Blueprint was reviewed to align with the current realities within the IT space in the Banking Industry.

The IT Standards Council set up and mandated the IT Standards Review committee to revise the Blueprint. The following activities were carried out during the revision process:

- Reviewed the current IT Standards Blueprint to identify gaps and opportunities for improvement
- Reviewed outcome of IT Standards Baseline Assessment
- Administered IT Standards Survey to the banks
- Gathered feedback on current IT Standards Blueprint from the CIO workshop
- Researched local and global current and emerging trends in IT for the FS industry and determined their relevance to current exercise

Outcomes from the above listed activities were taken into consideration in the development of the revised Blueprint.

1.2 **Revision of the IT Standards Blueprint**

The current Standards Blueprint was developed in 2010 and published by the Central Bank of Nigeria to the Banking Industry on January 16th, 2014. Within this period, certain Standards have become outdated, discontinued and replaced with other Standards. In addition, trends such as cloud computing, outsourcing/managed services, social media and big data have gained significant prominence. The IT Standards Blueprint was reviewed by the IT Standards Council to align it with the current realities within the IT space in the Banking Industry.

1.2.1 **Summary of Changes to the IT Standards Blueprint**

The table below presents a summary of changes made to the blueprint:

	Section	Change
1.	Sections 1.1 – 1.3	Updated the background and objectives in line with the current realities
2.	Sections 2.1 – 2.7	Included the Business justification for inclusion of Standards in each capability area in the Blueprint
3.	Section 2.1 – 2.7	Included the version of the Standards for which compliance is expected
4.	Section 2.4.1	Removed ISO 15504 as a Standard for Application Development. The Capability Maturity Model Integration (CMMI) will serve as the only Standard in this capability area
5.	Section 2.5.3	Revised the scope of the Occupational Health and Safety Management Systems standards (OHSAS 18001) to focus on IT locations and environments
6.	Section 2.5.4	Replaced the British Standard – BS 25999 on business continuity (the Standard has been retired) and replaced it with ISO 22301
7.	Section 2.6	Included new scope for ISO 27001/2 compliance
8.	Section 3.1	Revised priorities of Standards in the Blueprint
9.	Section 3.2	Revised implementation timeline/Standards adoption roadmap
10.	Section 4.1	Included considerations for IT Service Provider/Vendor Engagement
11.	Section 6.1	Included IT Trends and its implications for the Nigerian FS industry
12.	Formerly Section 4	Removed the section on IT Standards Governance and Interaction Model. This section is now a standalone document and is contained in the Terms of Reference for the IT Standards

	Section	Change
		Governance Council

Table 1: Summary of changes to the Blueprint

1.3 Objectives and Purpose of Document

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

- Objective and intention
- Description of the Standards
- Benefits to the Bank
- Requirements for compliance

Banks 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.

While the focus of the Blueprint is to drive process maturity, undergoing the certification process and obtaining certification(s) to the Standards in the Blueprint is seen as a step in journey towards achieving and maintaining process maturity and will not by itself suffice for the requirements on the acceptable minimum level of process maturity.

1.4 Definition of Standard

For the purposes of this document, a Standard is an established, measurable and achievable set of criteria agreed by general consent to be a basis of comparison.

1.5 Overview and Summary IT Standards for the Nigerian Banking Industry

The IT Standards Blueprint aims to help Nigerian Banking institutions develop capabilities under seven (7) key technology Capabilities areas. Skills in these capability areas would support in transforming the Banks' IT function to a world class, high

performing IT operations and also help to position it as a strategic asset to the Bank.

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.
IT Governance	Framework for initiation, endorsement, sponsorship, approval and evaluation of IT decisions
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
Workforce & Resource Management	Management of IT skills, knowledge and Banking resources

Table 2: IT Capability Areas

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

Capability		Standards	
Strategic IT Alignment		IT Infrastructure Library (ITIL)	Control Objectives for Information and related Technologies (COBIT)
IT Governance		COBIT	ISO 38500
Architecture & Information Management	Interfaces	ISO 8583	ISO 20022
	Reporting	eXtensible Business Reporting Language (XBRL)	
	Enterprise Architecture	The Open Group Architecture Framework (TOGAF)	
Solutions Delivery	Applications Development	Capability Maturity Model Integration for Development (CMMI - Dev)	
	Project Management	Project Management Body of Knowledge (PMBOK)	PRojects IN Controlled Environments version 2 (PRINCE2)
Service Management & Operations	Service Management	ITIL	ISO 20000
	Data Center	Tier Standards	TIA 942
	Health, Safety, Environment (HSE)	OHSAS 18001	
	Business Continuity	Business Continuity Institute Good Practice Guidelines (BCI GPG)	ISO 22301 [1]
Information & Technology Security	Payment Card Security	Payment Card Industry Data Security Standard (PCI DSS)	
	Information Security	ISO 27001/27002	
	Cyber Security	ISO 27001/27002 and Payment Card Industry Data Security Standard (PCI DSS)	
Workforce & Resource Management		Skills Framework for the Information Age (SFIA)	

Table 3: IT Capability Areas and IT Standards

[1] Formerly BS 25999 which was retired on September 1, 2012 and replaced by ISO 22301

1.6 **Target Maturity Levels**

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

The Blueprint drives the adoption of IT Standards. It encourages Banks to build capacity and embed mature IT processes within their organisational practices. Process maturity provides Banking Institutions the opportunity not only to improve their IT processes but to embed global leading IT practices within the organisation resulting in tangible, visible improvements.

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

While the Blueprint focuses on process maturity, it sees achieving certification on the IT Standards as a step in the journey towards process maturity. It is important to note however that achieving certification on a standard or set of standards does not suffice for the requirement for maintaining the requisite level of process maturity. Attainment of the required level of process maturity is evidenced by demonstrable proof that the IT processes and underlying controls have been embedded in the Bank's Information Technology practices.

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 disorganized
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 organizational 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 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 4: Definition of Maturity Levels

The minimum target maturity level for IT Standards for the Banking industry is Level 3 in respect of Standards that align to the maturity model.

Level 3 maturity requires that IT Standards are

- Defined
- Documented
- Integrated into organizational practices via policy and procedures
- Communicated through training, and that
- Automation and tools are used in a limited and fragmented way

The table below gives the detailed explanation of the expectations of a level 3 process maturity for each Standard

Categories	Description of Level 3 Maturity
Defined	• The processes prescribed by the Standard exists formally in the bank • The formal existence of a process is demonstrated by

	o The existence of a process owner, o Definite process steps and o Definite outcomes
Documented	• Processes are defined and formalised in a process documentation that has been signed off by the appropriate authority • At the minimum, process documentation should contain the following : o Objective o Scope o KPIs/Key success factors o Governance o Process activities o Roles and responsibilities o Interfaces with other processes o Reporting requirements o Controls for improving the process
Integrated into organizational practices via policy and procedures	• Existence of documented policies and procedures • Evidence that the process is being implemented within the organisation via artefacts such as reports, test scripts, lessons learned, etc. • Defined, documented and measured process interfaces
Communicated through training and upskilling of process resources	• Roles and responsibilities of resources participating in the execution of the process are properly defined and documented • Evidence of a training plan and/or schedule that is being implemented • Evidence of formalized knowledge transfer sessions • Subscription to relevant IT resources - journals and /or magazines • IT personnel possess relevant IT certifications like: ITIL, PRINCE2, PMP, CBCI, CDCMP, CISA, CISM, CISSP, etc.
Process Automated	• At least one tool is consistently used to automate the full process or some part of the process

Table 5: Description of Level 3 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 Banking 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 organization 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 your Bank and its IT organization • Clear expectations of IT, on how it will contribute to reaching the Bank'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 Bank'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	• Control Objectives for Information and Technology (COBIT): best practices for IT management, created by ISACA and the IT Governance Institute • IT Infrastructure Library (ITIL): globally adopted framework for IT Operations and Service Management
Version of the Standard to which	• COBIT 5.1 • ITIL 2011

Compliance is Required	
Minimum Acceptable Maturity Level	• Level 3
Rationale for Selection	**COBIT** COBIT 5.1 is based on a revised process reference model with a new governance domain and several new and modified processes that now cover enterprise activities end-to-end, i.e., business and IT function areas. The COBIT goal translates stakeholder needs into specific, practical and customized goals within the context of the enterprise, IT-related goals and enabler goals. COBIT 5 consolidates COBIT4.1, Val IT and Risk IT into a single framework acting as an enterprise framework aligned and interoperable with TOGAF and ITIL. **ITIL** 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. COBIT and ITIL are 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 COBIT Evaluate, Direct and Monitor (EDM) Domain and the ITIL Service Strategy volume maturity level 3. Strategic IT Alignment policies and processes must be: • Defined • Documented • Integrated into organizational practices via policy and procedures • Communicated through training

	• Processes must be automated to some degree The process for demonstrating compliance to COBIT and ITIL is as follows: • Implement the IT Strategy requirements of the COBIT /ITIL frameworks to maturity level 3 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 Banking industry including in-house Bank functions and external IT infrastructure and service providers
References	ITIL: http://www.itil-officialsite.com/ COBIT: http://www.isaca.org/Knowledge-Center/cobit

Key Elements of the Standards
Please see sections 2.2 and 2.5.

2.2 IT Governance

Purpose	The IT Governance Standard articulates a framework to guide how IT decisions are made, sponsored, enforced and evaluated, both within and across the organization structure
Justification	**Business Challenge** • Pressure to demonstrate to investors that the Bank is well run and is capable of delivering maximum returns to shareholders and customers • Difficulty in managing IT effectively • Increase in Cost and time effectiveness in customer service **How this Capability Addresses these Challenges** • IT Governance helps the Banks address these challenges by providing a framework for managing people, processes and resources. Ultimately the goal is to align the Bank's IT goals with its business goals to ensure optimum and uninterrupted service delivery. • IT Governance enables the Bank know what its resources are, who is using the resources, why they are using the resources and whether resources are being used in the most time- and cost-effective methods. • IT Governance covers the culture, organisation, policies and practices that provide an oversight and help to make IT more transparent. This not only reduces IT risk but also improves communication and ensures greater trust, teamwork and confidence in the use of IT itself and the people trusted with IT services **Business Benefits** • Improves business performance by effectively helping organizations manage and govern their information and technology • Helps assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes • Aids in embedding IT into the organization's culture • Helps in aligning IT with the organizational goals and strategy
Standards	• Control Objectives for Information and Technology (COBIT): a set of best practices for IT management, created by ISACA and the IT Governance Institute. • ISO 38500: created by the International Standards Organization; focuses on the corporate governance of information technology
Version of the Standard	• COBIT 5.1

to which Compliance is Required	• ISO/IEC 38500:2015
Maturity Level	• Level 3
Rationale for Selection	**COBIT** The COBIT Framework provides management and business process owners with an IT governance model that helps in delivering value from IT as well as managing the risks associated with IT. **ISO 38500** The ISO/IEC 38500 Standard provides a framework for effective governance of IT to assist those at the highest level of organization to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organization's use of IT. The Standard specifies the minimum requirements for the IT Governance of an organization. COBIT and ISO 38500 are complementary– implementation of COBIT controls satisfy some of the requirements for ISO 38500
Benefits	• Improved accountability for IT investments • Higher level of business justification for IT projects • Increased effectiveness of the IT function leading to reduction in costs • Improved risk management with better visibility of risk priorities
Requirements for compliance	COBIT: In order to be compliant to the industry Standard, the COBIT framework must be implemented to maturity level 3. This means that the Standard must be: • Defined • Documented • Integrated into organizational practices via policy and procedures • Communicated through training • Processes must be automated to some degree ISO 38500: The ISO 38500 requirements must be met for an organization to be compliant to this Standard

	The processes for an organization to become compliant to COBIT and ISO 38500 are as follows: COBIT • Implement the requirements of the COBIT framework to maturity level 3 and submit to a formal assessment by the IT Standards Council • If all requirements are met, the organization will be deemed to have complied by the IT Standards Governance Council. ISO 38500 • Implement the requirements of the ISO 38500 Standard • Submit to a formal assessment by the IT Standards Council by a certified assessor. • Provide the results to the IT Standards Governance Council as proof of compliance
Scope	This Standard is applicable to all the Banks and managed service providers in the industry. • All organizations in the industry shall implement the COBIT framework to maturity level 3.

Key Elements of the Standards

COBIT:

The COBIT 5 processes are split into governance and management "areas". These 2 areas contain a total of 5 domains and 37 processes:

- Governance of Enterprise IT
  - Evaluate, Direct and Monitor (EDM) – 5 processes
- Management of Enterprise IT
  - Align, Plan and Organise (APO) – 13 processes
  - Build, Acquire and Implement (BAI) – 10 processes
  - Deliver, Service and Support (DSS) – 6 processes
  - Monitor, Evaluate and Assess (MEA) - 3 processes

The domains map to the IT function's traditional responsibility areas of plan, build, run and monitor

Evaluate, Direct and Monitor (EDM)	Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against agreed-on direction and

	objectives
Align, Plan and Organize (APO)	The Align, Planning and Organization domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT.
Build, Acquire and Implement (BAI)	The Build, Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes.
Deliver, Service and Support (DSS)	The Deliver, Service and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as, the support processes that enable the effective and efficient execution of these IT systems.
Monitor, Evaluate and Assess (MEA)	The Monitor, Evaluate and Assess domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors.

Ref: http://www.isaca.org/COBIT/Pages/default.aspx

ISO 38500

ISO 38500 is a high level principle based advisory Standard. In addition to providing broad guidance on the role of a governing body, ISO 38500 encourages organizations to use appropriate Standards to underpin governance of IT.

The Standard prescribes that directors should govern IT through three main tasks:

- Evaluate the current and future use of IT
- Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives
- Monitor conformance to policies, and performance against plans.

There are six principles for good corporate governance of IT. The principles are applicable to organizations and express preferred behaviour to guide decision making. The statement of each principle refers to what should happen but does not prescribe how, when or by whom the principles should be implemented.

- Principle 1- Responsibility: Individuals and groups across the organization understand and accept their responsibilities in respect of supply of and demand for IT. Responsibility is matched by authority to perform.
- Principle 2 - Strategy: Corporate business strategy reflects current and future capabilities of IT. IT strategy and plans are clearly articulated and are aligned to and supportive of current and ongoing needs of the organization's Business strategy.
- Principle 3 - Acquisition: IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis with clear and transparent decision making. There is appropriate consideration of short and long term benefits, opportunities, costs and risks of IT spend.
- Principle 4 - Performance: IT is fit for purpose in supporting the organization, providing services levels and service quality appropriate for current and future business requirements
- Principle 5 - Conformance: IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
- Principle 6 – Human Behaviour: IT policies, practices and decisions demonstrate respect for human behaviour including the current and evolving needs of all people in the process.

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

2.3 Architecture and Information Management

2.3.1 **Interfaces**

Purpose	The purpose is to ensure the Standardization of transaction interfaces between entities in the Banking 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 Banking 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 3
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 Banking industry for card based payment transactions. **ISO 20022** Also known as the Universal Banking 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
Requirements for compliance	Transaction interfaces that meet specified industry Standards. **Process 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 organization will be deemed to have complied by the IT Standards Council
Scope	This Standard is applicable to all banks, managed service providers and payments systems solution providers in the industry. • All organizations that provide payments services are required to provide ISO 8583 compliant interfaces.

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 Banking 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/

2.3.3 Reporting

Purpose	Standardization of business and Banking 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)
Maturity Level	• Level 3
Version of the Standard to which Compliance is Required	• XBRL 2.1
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 can assembled quickly, cheaply and efficiently • Improved usability of Banking statement information • Simplification of both internal and external reporting processes
Requirements for compliance	In order to be compliant, an organization 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 organization will be deemed to have complied by the IT Standards Governance Council
Scope	This Standard is applicable to all banks and external (managed) service providers for the Banking industry.

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: o 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. o 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 of time 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

2.3.4 Enterprise Architecture

Purpose	Enterprise architecture Standard provides a framework to guide the selection, deployment, operation, protection and refreshment of technologies in support of business goals
Justification	**Business Challenge** • Failure in planning to meet the needs of internal customers • Overwhelming application maintenance **How this Capability Addresses these Challenges** • Enterprise architecture brings IT close to the internal customer by getting first-hand knowledge of what internal customers are saying and to translate into IT projects. It balances the technical viability of product solutions while determining their economic value to the business. • Enables Banks' to build architecture that aligns and integrates business concerns (people, processes, technologies, and infrastructures) and information systems architectures (data and applications) in an elegant, robust manner by: o Identifying gaps in current capability. Plugging these, the enterprise can become more effective and efficient o Optimizing processes to reduce time to market **Business Benefits** • Supports Banking Institutions in achieving the right balance between IT efficiency and business innovation by allowing individual business units to innovate safely in their pursuit of competitive advantage o Eliminating duplication in applications, projects, infrastructure etc. o Making implementations more efficient through Standards, reuse and interoperability etc. o Providing an optimized view of IT demand for software, hardware and services. This can then power effective procurement through strategic sourcing Helps IT operate more efficiently by: • Lowering software development, support, and maintenance costs • Increasing portability of applications o Improves interoperability and easier system and network management and the ability to address critical enterprise-wide issues like security o Develops practices that ensure accountability to a clearly identified stakeholder community, both inside and outside the organization

Standard	• The Open Group Architecture Framework (TOGAF)
Version of the Standard to which Compliance is Required	• TOGAF V 9.1
Maturity Level	• Level 3
Description of Standards	• TOGAF is an architecture framework that provides a set of tools which can be used for developing a broad range of different architectures
Rationale for Selection	• TOGAF is a framework that includes a comprehensive set of supporting tools for the design, planning, implementation, and governance of an enterprise architecture. • It is the most widely adopted open framework for Enterprise Architecture in Nigeria and in most parts of the world
Benefits	• The TOGAF Architecture Development Method (ADM) provides a detailed methodology that can enable the development of an enterprise architecture which will meet the business and information technology needs of an organization. • The ADM is freely available for use by any organization to develop an enterprise architecture for use within that organization alone, and is customizable to meet the organization's needs.
Requirements for compliance	In order to be compliant to the industry Standard the TOGAF framework must be implemented to maturity level 3. This means that the Standard must be: • Defined • Documented • Integrated into organizational practices via policy and procedures • Communicated through training • Processes must be automated to some degree **Process for compliance** • Implement the requirements of the TOGAF framework to maturity level 3 and submit to a formal assessment by the IT Standards Council

	• If all requirements are met, the organization will be deemed to have complied by the IT Standards Governance Council
Scope	This Standard shall be applicable to all banks and external (managed) service providers in the Banking service industry.
References	TOGAF: http://www.opengroup.org/togaf/

Key Elements of the Standards

The TOGAF Architecture Development Method (ADM) is a framework for developing an enterprise architecture covering Business Architecture, Application Architecture, Information Architecture and Technology Architecture. The TOGAF ADM consists of a number of phases that cycle through all the architecture views as follows:

- Preliminary Framework and Principles: focuses on establishing the business context, defining framework to be used, defining architecture principles and establishing architecture governance
- Architecture Vision: obtain management commitment towards project(s), validate the business principles, goals and drivers, identify stakeholder concerns and objectives, define business requirements and constraints and obtain formal approval to proceed.
- Business Architecture: describe the current baseline business architecture, develop a target business architecture and analyze the gaps between the baseline and target business architectures.
- Information Systems Architecture: develop target architectures for data and application domains. The scope of business process supported in this phase includes those that are supported by IT and the interfaces of IT related processes to non IT related processes. It consists of
  - Data Architecture: which aims to define the types and sources of data needed to support the business in a way that can be understood by stakeholders
  - Applications Architecture: which aims to define the kinds of application systems necessary to process the data and support the business.
- Technology Architecture: develop a technology architecture that supports the business, application and data architectures
- Opportunities and Solutions: evaluate and select implementation options, identify the strategic parameters for change and the projects to be undertaken and generate an implementation and migration strategy and plans.
- Migration Planning: plan various implementation projects by priority. The prioritized list of projects will form the basis for the detailed implementation and migration plans.
- Implementation Governance: arrangements for conformance with the defined architecture by the implementation projects and other projects.
- Architecture Change Management: continual monitoring of changes in technology and business to determine whether to initiate a new architecture cycle.

Ref: http://www.opengroup.org/togaf/

2.4 Solutions Delivery

2.4.1 Applications Development

Purpose	The purpose of these Standard is to ensure that there is a structured process for the development of bespoke applications or the customization of commercial applications as required by the organization.
Justification	**Business Challenge** • Complexities of software application development is significantly increasing, the technologies of programming languages are rapidly changing, and the design patterns and tools are constantly being modified • The lack of good process practices/guidelines for software development organization **How this Capability Addresses the business Challenges** • CMMI – Dev ensures better management of application development by providing a means for quality assurance, reduction in the cost of maintenance, as well as establishment of control for process improvement **Business Benefits** • Helps organization achieve process improvement on software development processes which in turn increases return on investment • Delivers real cost savings by effectively detecting error early, and hence reduces cost of remediation
Standards	• Capability Maturity Model Integration for Development (CMMI – Dev) is a process improvement method that provides a set of best practices for Systems and Software development
Version of the Standard to which Compliance is Required	• CMMI – Dev Version1.3
Maturity Level	• Level 3
Rationale for Selection	**CMMI – Dev** The CMMI – Dev is a Framework for projects or organizations that provides common, integrated, and improving processes for Systems and Software development. It provides a set of best practices that address productivity, performance, costs, and stakeholder satisfaction and can be utilized to drive significant value realization.

Benefits	• Better ROI indices for application development initiatives • Improved quality of end deliverables with reduced defects over product life cycle • Reduction in project costs with reduced schedules • Improved end-user satisfaction
Requirements for compliance	CMMI - Dev: In order to be compliant to the industry Standard the CMMI model must be implemented to maturity level 3 as defined **Process for compliance** CMMI - Dev: • Implement the requirements of the CMMI Model to maturity level 3 and submit to a SCAMPI formal assessment by the IT Standards Council by a QSA • If all requirements are met, the organization will be deemed to have complied by the IT Standards Council.
Scope	This Standard is applicable to all the banks and external (managed) service providers in Banking industry. • All organizations in the industry are required to implement CMMI - Dev to at least a maturity level three

Key Elements of the Standards

CMMI - Dev:

CMMI for applications development consists of 22 process areas. A process area is a cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making significant improvement in that area. These process areas are aligned to maturity levels and determine the level of maturity of an organization's development processes. The process areas are as follows:

Maturity Level 2 – Managed:

- CM - Configuration Management: establish and maintain the integrity of work products using configuration identification, configuration control, configuration status accounting, and configuration audits.
- MA - Measurement and Analysis: develop and sustain a measurement capability used to support management information needs.
- PMC - Project Monitoring and Control: provide an understanding of the project's progress so that appropriate corrective actions can be taken when the project's performance deviates significantly from the plan
- PP - Project Planning: establish and maintain plans that define project activities.
- PPQA - Process and Product Quality Assurance: provide staff and management with objective insight into processes and associated work products.
- REQM - Requirements Management: manage requirements of the project's products and product components and to ensure alignment

between those requirements and the project's plans and work products.

- SAM - Supplier Agreement Management: manage the acquisition of products and services from suppliers

Maturity Level 3 - Defined

- DAR - Decision Analysis and Resolution: analyze possible decisions using a formal evaluation process that evaluates identified alternatives against established criteria.
- IPM - Integrated Project Management: establish and manage the project and the involvement of relevant stakeholders according to an integrated and defined process that is tailored from the organization's set of Standard processes.
- OPD - Organizational Process Definition: establish and maintain a usable set of organizational process assets, work environment Standards, and rules and guidelines for teams.
- OPF - Organizational Process Focus: plan, implement, and deploy organizational process improvements based on a thorough understanding of current strengths and weaknesses of the organization's processes and process assets.
- OT - Organizational Training: develop skills and knowledge of people so they can perform their roles effectively and efficiently.
- PI - Product Integration: assemble the product from the product components, ensure that the product, as integrated, behaves properly (i.e., possesses the required functionality and quality attributes), and deliver the product
- RD - Requirements Development: elicit, analyze, and establish customer, product, and product component requirements.
- RSKM - Risk Management: identify potential problems before they occur so that risk handling activities can be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives.
- TS - Technical Solution: select, design, develop, and implement solutions to requirements. Solutions, designs, and implementations encompass products, product components, and product related lifecycle processes either singly or in combination as appropriate.
- VAL – Validation: demonstrate that a product or product component fulfills its intended use when placed in its intended environment.
- VER – Verification: ensure that selected work products meet their specified requirements.

Maturity Level 4 - Quantitatively Managed

- OPP - Organizational Process Performance: establish and maintain a quantitative understanding of the performance of selected processes in the organization's set of Standard processes in support of achieving quality and process performance objectives, and to provide process performance data, baselines, and models to quantitatively manage the organization's projects.
- QPM - Quantitative Project Management: quantitatively manage the

project to achieve the project's established quality and process performance objectives.

Maturity Level 5 - Optimizing

- CAR - Causal Analysis and Resolution: identify causes of selected outcomes and take action to improve process performance.
- OPM - Organizational Performance Management: proactively manage the organization's performance to meet its business objectives.

Ref: http://www.sei.cmu.edu/cmmi/

2.4.2 Project Management

Purpose	The Project Management Standard provide 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 organization competitive edge, by ensuring that organizations project management strategies directly aligns with the strategic business goals • Ensures Standard processes is 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	• PRINCE2:2009

to which Compliance is Required	• PMBOK Guide – Fifth Edition (2013)
Maturity Level	• Level 3
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 organization 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 increase on-schedule project delivery
Requirements for compliance	In order to be compliant to the industry Standard, the PMBOK or PRINCE2 framework must be implemented to maturity level 3. This means that the Standard must be: • Defined • Documented • Integrated into organizational practices via policy and procedures • Communicated through training • Processes must be automated to some degree **Process for compliance** • Implement the requirements of the PMBOK/PRINCE2 Standards to maturity level 3 and submit to a formal assessment by the IT Standards Council • If all requirements are met, the organization will be deemed to have complied by the IT Standards Council.
Scope	The Project Management Standard shall be applicable to all the banks and external (managed) service providers

	in the industry. • Organizations are required to implement either the PMBOK or PRINCE2 Standards to at least a maturity level 3

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: http://www.prince-officialsite.com/

2.5 Service Management and Operations

2.5.1 Service Management

Purpose	The purpose of this Standard is to ensure that there is a structured framework for managing the development and delivery of IT Services.
Justification	**Business Challenge** • High cost of IT and difficulties in value derivation from IT investment • While IT solutions are introduced via a project, the business derives value from IT applications/systems in live operation. However it is often challenging for banks because most often the systems transitioned to operations do not actually solve the business challenge for which they were intended • The projects fail to deliver value because they are

	not properly planned, designed, implemented or received **How this Capability Addresses the business Challenge** • For an IT investment to deliver its potential value, the resulting IT service must be well planned, designed, implemented, delivered, and received. This is what IT Service Management seeks to achieve **Business Benefits** • IT Service management enables Banking Institutions plan, design, develop, deliver and optimize IT services that are both fit for purpose and fit for use - thus ensuring value and return on investment can be maximised
Standards	• IT Infrastructure Library (ITIL) is a framework of best practice for IT service management. It comprises a series of books and information which provide guidance on the quality provision of IT services. • ISO 20000 is an organizational Standard that aims to promote the adoption of an integrated set of management processes for the effective delivery of services to the business and its customers
Version of the Standard to which Compliance is Required	• ITIL 2011 • ISO/IEC 20000-1:2011
Maturity Level	• Level 3
Rationale for Selection	**ITIL** ITIL is a framework of best practices for IT service management which gives detailed descriptions of IT processes and provides comprehensive checklists, tasks and procedures that any IT organization can tailor to its needs. **ISO 20000** This is an international Standard that defines the requirements for an organization to deliver services of an acceptable quality to its customers. It aims to promote the adoption of an integrated set of management processes for the effective delivery of services to the business and its customers ITIL and ISO 20000 are complementary to one another – implementing ITIL processes satisfy some of the requirements towards attaining an ISO 20000 certification

Benefits	• Improved quality and consistency of IT Services • Improved alignment of IT Services with corporate strategies and all aspects of existing technologies, processes and services leading to reduced Total Cost of Ownership (TCO) • Structured service design processes enabling IT to focus on delivering cost effective services while ensuring that specific business requirements are met • Provides a basis for independent assessment of IT Service Management processes
Requirements for compliance	ITIL: in order to be compliant to the industry Standard the ITIL framework must be implemented to maturity level 3. This means that the Standard must be: • Defined • Documented • Integrated into organizational practices via policy and procedures • Communicated through training • Processes must be automated to some degree ISO 20000: the ISO 20000 requirements must be met and certification obtained for an organization to be compliant to this Standard. **Process for compliance** ITIL: • Implement the requirements of the ITIL Standard to maturity level 3 and submit to a formal assessment by the IT Standards Council • If all requirements are met, the organization will be deemed to have complied by the IT Standards Council. ISO 20000 • Implement the requirements of the ISO 20000 Standard • Request an assessment from a Registered Certification Body (RCB). Once the requirements of ISO/IEC 20000 have been satisfied, the RCB will issue a certificate of conformance • Provide the certificate to the IT Standards Council as proof of compliance
Scope	This Standard is applicable to all the banks and external (managed) service providers in the Banking industry.

	• All organizations in the industry are required to implement the ITIL framework to at least a maturity level 3

Key Elements of the Standards

ITIL:

Current ITIL version is ITIL 2011which is an update to version 3 (ITIL 2007) with no significant changes in context consists of five core publications covering each stage of the service lifecycle from the initial definition and analysis of business requirements in Service Strategy and Service Design, through migration into the live environment within Service Transition, to live operation and improvement in Service Operation and Continual Service Improvement

- Service Strategy: this publication sits at the core of the ITIL V3 lifecycle. It sets out guidance to all IT service providers and their customers, to help them operate and thrive in the long term by building a clear service strategy
- Service Design: The purpose of this is the design of appropriate and innovative IT services, including their architectures, processes, policies and documentation, to meet current and future agreed business requirements.
- Service Transition: this aims to deliver services that are required by the business into operational use. Service Transition delivers this by receiving the Service Design Package from the Service Design stage and delivering into the Operational stage every necessary element required for ongoing operation and support of that service.
- Service Operation: the purpose is to deliver agreed levels of service to users and customers, and to manage the applications, technology and infrastructure that support delivery of the services. It is only during this stage of the lifecycle that services actually deliver value to the business, and it is the responsibility of Service Operation staff to ensure that this value is delivered.
- Continual Service Improvement: this is concerned with maintaining value for customers through the continual evaluation and improvement of the quality of services and the overall maturity of the ITSM service lifecycle and underlying processes. CSI combines principles, practices and methods from quality management, Change Management and capability improvement, working to improve each stage in the service lifecycle, as well as the current services, processes, and related activities and technology.

ITIL: http://www.itil-officialsite.com/

ISO 20000

The ISO 20000 Standard specifies a set of inter-related management processes and is derived from ITIL. ISO 20000 requires an integrated process approach for the effective provision of IT services and includes

the relationship with customers and suppliers as part of its evaluation.

The Standard consists of two parts: The Specification ISO20000-1 defines the requirements for a service provider to deliver managed services, while the Code of Practice ISO20000-2 describes detailed best practices for the processes defined within ISO 20000-1. Overall, ISO 20000 specifies five key group service management processes: Service Delivery, Relationship, Resolution, Control and Release.

ISO 20000 uses the same approach as management system Standards such as ISO 9001 and ISO 27001, including the PDCA (Plan-Do-Check-Act) methodology. ISO 20000 mandates the application of "Plan-Do-Check-Act" (PDCA) to all parts of the Service Management System (SMS) and the services. The PDCA methodology, as applied to ISO 20000 consists of the following:

- **Plan**: establishing, documenting and agreeing the SMS. The SMS includes the policies, objectives, plans and processes to fulfil the service requirements.
- **Do**: implementing and operating the SMS for the design, transition, delivery and improvement of the services.
- **Check**: monitoring, measuring and reviewing the SMS and the services against the policies, objectives, plans and service requirements and reporting the results.
- **Act**: taking actions to continually improve performance of the SMS and the services.

The PDCA methodology helps to achieve the following:

- understanding and fulfilling the service requirements to achieve customer satisfaction;
- establishing the policy and objectives for service management;
- designing and delivering services based on the SMS that add value for the customer;
- monitoring, measuring and reviewing performance of the SMS and the services;
- continually improving the SMS and the services based on objective measurements

The Standard promotes an integrated service management model comprising of the following:

- Requirements for a Management System
    - Management Responsibility
    - Documentation requirements
    - Competence, awareness and training
- Planning and Implementation of Service Management
    - Plan service management
    - Implement service management and provide the services
    - Monitoring, measuring and review
    - Continual Improvement

- Planning and Implementing new or changed services
- Service Delivery Processes
    - Service Level Management
    - Service Reporting
    - Service Continuity and Availability Management
    - Budgeting and Accounting for IT Services
    - Capacity Management
    - Information Security Management
- Relationship Processes
    - General requirements
    - Business Relationship Management
    - Supplier Management
- Resolution Processes
    - Background
    - Incident Management
    - Problem Management
- Control Processes
    - Configuration Management
    - Change Management
- Release Processes
    - Release Management

ISO 20000: http://www.iso.org/

2.5.2 Data Centre

Purpose	Standard for infrastructure and communication for data processing sites for the Banking industry
Justification	**Business Challenge** • Increase in data center budget • Lack of adequate knowledge of the different systems and applications which causes disruption during migration and hence impacts business continuity • Difficulty in aligning data center infrastructure with disaster recovery **How this Capability Addresses these Challenges** • Ensures end-to-end application management which includes tools for rapid application discovery, managing dependencies and business ownership across data center which increases control **Business Benefits** • Increases application availability and operating efficiency by ensuring that the right applications are placed on the right hardware and the applications are optimizing the resources assigned to them • Reduces cost, risks and environmental Impacts which helps the organization free up about 50 percent of its IT budget while also lowering carbon footprint • Reduces failure cost by cutting down downtime cost per minute which in turn increases availability time • Provides visibility into the physical infrastructure which informs administrators “at-a-glance” how their data center environment is configured, what resources are assigned to which physical or virtual servers and how the consumption of those resources is changing • Reduces unplanned failures and improves overall performance by not being susceptible to disruption from planned site maintenance
Standards	• The Uptime Institute Tier Standard is a global Standard based on availability specifications for Data centres • TIA 942 Standard for Data centres is a telecommunications Standard that specifies requirements for telecommunications infrastructure and facilities of Data centres
Version of the Standard	• TIA 942 : Data Centre April 2013

to which Compliance is Required	
Acceptable Tier	• Tier 3
Rationale for Selection	**Data Centre Tier Standard** The Uptime Institute site infrastructure tier Standard is a widely adopted global Standard that was developed as an objective basis for comparing the functionality, capacity and expected availability of a data center site **TIA 942 Standard** The Telecommunications Infrastructure Standard for Data Centres specifies the minimum requirements for telecommunications infrastructure and facilities of Data centres and computer rooms including single tenant enterprise Data centres and multi-tenant Internet hosting Data centres. The Standard is primarily a telecom infrastructure Standard, but also addresses data center facility requirements as follows: • Site space and layout • Cabling infrastructure • Tiered reliability • Environmental considerations
Benefits	Implementation of these Standards is expected to provide the following benefits: • Increased up-time / availability of Banks leading to increased cost savings • Establishment of a reference point for objective assessment of the IT function leading to improved IT performance measurement • Improved data integrity and electronic information exchange • Increased efficiency and productivity of staff due to interoperability of IT systems • Business Continuity / Recovery and reduced risk of prolonged downtimes • Improved data security assurance to customers leading to increased customer confidence
Requirements for compliance	In order to be found compliant, an organization's data center must meet the requirements for Tier 3 Data centre as defined. **Process for compliance** • Upgrade data center to meet Tier 3 requirements.

	• Notify the IT Standards Council of formal assessment by the IT Standards Council readiness • Submit to formal assessment by the IT Standards Council • If all requirements are met, the organization will be deemed to have complied by the IT Standards Council
Scope	This Standard shall be applicable to all banks and external (managed) service providers in the Banking industry. All data center infrastructure and facilities for the Nigerian FS industry shall satisfy the requirement for tier 3.

Key Elements of the Standards

Uptime Institute Tier Standard:

The tier Standard establishes four distinctive definitions of data center site infrastructure Tier classifications (Tier I, Tier II, Tier III, Tier IV), and the performance confirmation tests for determining compliance to the definitions. The Tier classifications describe the site-level infrastructure topology required to sustain data center operations, not the characteristics of individual systems or subsystems. The Tiers are as follows:

- Tier I - Basic Site Infrastructure: A Tier I basic data center has non-redundant capacity components and a single, non-redundant distribution path serving the computer equipment.
- Tier II - Redundant Site Infrastructure Capacity Components: A Tier II data center has redundant capacity components and a single, non-redundant distribution path serving the computer equipment.
- Tier III - Concurrently Maintainable Site Infrastructure:
    - A Concurrently Maintainable data center has redundant capacity components and multiple independent distribution paths (power, cooling, network, etc.) serving the computer equipment. Only one distribution path is required to serve the computer equipment at any time. (one active, one alternate)
    - Each and every capacity component and element in the distribution paths can be removed from service in a planned basis without impacting any of the computer equipment.
    - Tier III engine generator systems are considered the primary power source for the data center. The local power utility is an economic alternative. Disruptions to the utility power are not considered a failure but rather an expected operational condition for which the site must be prepared. The engine generator system along with its power paths and other supporting elements (emergency power off, isolation valves, start system for engine generators, control system for mechanical plants etc.) must be concurrently maintainable

- Annual maintenance shutdowns are not required and unplanned failures are reduced to 1.6 hours on an annual basis (99.98% availability)
- All IT equipment is dual powered as defined by the Institute's Fault Tolerant Power Compliance Specification, Version 2.0 and installed properly to be compatible with the topology of the site's architecture. Transfer devices, such as point-of-use switches, must be incorporated for computer equipment that does not meet this specification

- Tier IV - Fault Tolerant Site Infrastructure:
  - A Fault Tolerant data center has multiple, independent, physically isolated systems that provide redundant capacity components and multiple, independent, diverse, active distribution paths simultaneously serving the computer equipment. The redundant capacity components and diverse distribution paths shall be configured such that "N" capacity is providing power and cooling to the computer equipment after any infrastructure failure.
  - All IT equipment is dual powered as defined by the Institute's Fault Tolerant Power Compliance Specification, Version 2.0 and installed properly to be compatible with the topology of the site's architecture. Transfer devices, such as point-of-use switches, must be incorporated for computer equipment that does not meet this specification.
  - Complementary systems and distribution paths must be physically isolated from one another (compartmentalized) to prevent any single event from simultaneously impacting either systems or distribution paths.
  - Continuous Cooling must be provided.

The Uptime Institute Tier Standard: http://www.uptimeinstitute.org

TIA 942

Intended for use by data center designers early in the building development process, and covers the following:

- Site space and layout: Proper space allocation for a data center starts with ensuring that space can be easily reallocated to changing environments and growth. Designers must strike a balance between acceptable initial deployment costs and anticipated space required in the future. The data center should be designed with plenty of flexible "white space," empty space that can accommodate future racks or cabinets. The space surrounding the data center must also be considered for future growth and planned for easy annexation. The Standard also recommends specific functional areas, which helps to define equipment placement based on the Standard hierarchical star topology design for regular commercial spaces.

  The TIA-942 specifies that a data center should include the following key functional areas:
  - One or More Entrance Rooms
  - Main Distribution Area (MDA)

- One or More Horizontal Distribution Areas (HDA)
- Equipment Distribution Area (EDA)
- Zone Distribution Area (ZDA)
- Backbone and Horizontal Cabling

- Cabling infrastructure: the Standard specifies a generic, permanent telecommunications cabling system and provides specifications for the following recognized cabling media:
  - Standard single mode fiber
  - 62.5 and 50µm multimode fiber
  - Laser-optimized 50µm multimode fiber
  - 75-ohm coaxial cable (recommended for E-1, E-3, and T-3 circuits)
  - 4-Pair Category 6 UTP and ScTP cabling
  - For horizontal cabling, the TIA-942 Standard recommends installing the highest capacity media available to reduce the need for re-cabling in the future.
- Tiered reliability: To provide a means for determining specific data center needs, the TIA-942 Standard includes information on data center availability tiers. These tiers are based on the Uptime Institute.
- Environmental considerations: Environmental considerations within the TIA-942 include
  - fire suppression,
  - humidity levels,
  - operating temperatures,
  - Architectural, electrical and mechanical system specifications.

  The requirement in respect of each environmental consideration is defined based on levels of reliability.

TIA 942 Standard for Data Centres: http://www.tiaonline.org/

The following tier levels are adapted from the TIA 942 and Uptime Institute Tier Standards:

Tier	Description	Characteristics of Tier
1	Basic Data Centre Site Infrastructure	▪ Numerous single points of failure in all aspects of design ▪ Generally unable to sustain more than a 10 minute power outage
2	Redundant Site Infrastructure Capacity Components	▪ Some redundancy in power and cooling systems ▪ Generator backup ▪ Able to sustain 24 hour power outage ▪ Minimal thought to site selection ▪ Vapour barrier ▪ Formal data room separate from other areas
3	Concurrently Maintainable Site Infrastructure	▪ Two utility paths (active and passive) ▪ Redundant power and cooling systems ▪ Redundant service providers ▪ Able to sustain 72-hour power outage ▪ Careful site selection planning ▪ One-hour fire rating ▪ Allows for concurrent maintenance
4	Fault Tolerant Site Infrastructure	▪ Two independent utility paths ▪ Independently dual-powered cooling systems ▪ Able to sustain 96 hour power outage ▪ Stringent site selection criteria ▪ Minimum two-hour fire rating ▪ 24/7 onsite maintenance staff

Target tier is **Tier 3:** Concurrently Maintainable Site Infrastructure and supports 99.982% availability.

2.5.3 Health, Safety and Environment

Purpose	Structured framework for ensuring a safe work environment
Standard	• BS OHSAS 18001
Version of the Standard to which Compliance is Required	• OHSAS 18001
Minimum Acceptable Maturity Level	• Level 3
Description of Standards	• BS OHSAS 18001 is a globally recognized framework for Occupational Health and Safety Management Systems (OHSMS)
Rationale for Selection	**BS OHSAS 18001** • BS OHSAS 18001 is one of the most recognized frameworks for occupational health and safety management systems that allows an organization to proactively control health and safety risks and improve performance. It provides an assessment specification for Occupational Health and Safety Management Systems. • While this is not an IT driven Standard, occupational safety is critical and is a key metric globally used in the appraisal of service providers across industries.
Benefits	• Demonstration to stakeholders of commitment to health and safety • Potential reduction in the number of accidents leading to a reduction in downtime and associated costs • Improved management of health and safety risks
Requirements for compliance	An organization must implement the necessary controls to meet the requirements of the OHSAS Standard and be certified by accredited OHSAS auditors. **Process for compliance** • Implement a Health and Safety Management System to meet the requirements of the OHSAS Standard • Submit to a formal assessment by the IT Standards Council by OHSAS auditors.

	• Provide a certificate of compliance to the IT Standards Council as proof of compliance
Scope	This Standard shall be applicable to all Data Centers, Server rooms and IT equipment rooms of the Banks and their branches.

Key Elements of the Standards

OHSAS 18001:

- Occupational Health & Safety (OH&S) Policy: Creation of an OH&S policy
- Planning
  - Hazard identification, Risk Assessment and Determining Controls
  - Legal and Other Requirements: Procedure for describing how legal information is identified and accessed.
  - Objectives and Programs: Outlines the importance of a process to manage OH&S programs with objectives & targets which are consistent with the policy
- Implementation and Operation
  - Resources, Roles, Responsibility, Accountability and Authority: Top management needs to take ultimate responsibility for health and safety. This requirement defines relevant management, accountability, structure, roles, responsibilities, authorities and includes the appointment of an OH&S management representative
  - Competence, Training, and Awareness: Ensures that persons performing tasks are competent and trained to do them
  - Communication, Participation and Consultation: Outlines required procedures for internal & external communications.
  - Documentation: Occupational Health and Safety Management Systems (OHSMS) documentation requirements in electronic or paper form
  - Control of Documents: Explains the requirement to control documents so that current versions are distributed and available at points of use and obsolete versions are removed from the system.
  - Operational Control: Identifies critical functions associated with the identified hazards where controls are necessary.
  - Emergency Preparedness and Response: Process required for identifying & responding to emergencies.
- Checking and Corrective Action
  - Performance Measurement and Monitoring: Measures data for action and describes the plan to monitor and measure OH&S performance on a regular basis.

- Evaluation of Compliance: Procedure(s) required for scheduled evaluations of compliance. The organization will need to keep records of these periodic evaluations.
- Incident Investigation, Non-conformances, Corrective & Preventive Action: Procedures for investigating incidents and acting on health and safety non-conformances. Corrective and Preventive actions must be taken.
- Control of Records: Records necessary to demonstrate conformity to the requirements of the OHSMS must be controlled
- Internal Audit: Procedure to conduct the audits of the OHSMS at planned intervals to ensure that the system complies with planned arrangements.

- Management review: Top Management must review the OHSMS at planned intervals to ensure that the system continues to be suitable, adequate and effective.

Ref: http://www.bsigroup.com/

2.5.4 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 Banking 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 Banking 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 organization 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 3
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 Organization's Culture o Understanding the Organization 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: In order to be compliant to the industry Standard the guidelines of the BCI GPG must be implemented within the organization. ISO 22301: In order to be compliant, the organization 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 organization 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 banks and external (managed) service providers in the Banking industry. • All organizations shall implement either the BCI GPG or the ISO 22301 guidelines

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
  - Policy and Programme Management: The BCM Policy of an organization 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
  - Embedding BCM in the Organization'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 Organization's Culture
    - Monitoring Cultural Change
- Technical Professional Practices
  - Understanding the Organization: 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 organization'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 organization 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.thebci.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 organization.
- Implementing and Operating the BCMS (DO): This focuses on the actual implementation of the plans. This section includes a number of 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

2.6 Information & Technology Security

2.6.1 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 your organizational information are secure and that you have 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 organizations 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 3.0
Acceptable Maturity Level	• Level 3

Rationale for Selection	**ISO 27001/27002** • ISO 27001 enables organizations 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 organization. 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 organizations 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: In order to be found compliant, the organization 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 organization 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 banks and external (managed) service providers in the industry. • PCI DSS compliance is mandatory for all organizations 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 organization 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 organization 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** o Information assets on the internet: websites , internet banking applications, apps, information assets in the cloud and social media **Business Continuity (Optional)** o 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 o 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 o 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

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
- Organization 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/

2.6.2 Cyber Security

Purpose	Cyber Security Standards helps banks to defend the customer and organizational 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 banks maintain their risk profile at an acceptable level
Justification	**Business Challenge** • Cyber-crimes are increasing in scope and sophistication at a time when banks are moving their key assets and systems to digital spheres and internet usage is growing significantly • Each year banks 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 banks **How this Capability Addresses these Challenges** • Complying with the Information Security Standards is one way to prove that your Bank is taking cyber security threats seriously • Compliance enhances the bank'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 and • PCI DSS

Version of the Standard to which Compliance is Required	• ISO/IEC 2700/21:2013; • PCI-DSS Version 3.0
Minimum Acceptable Maturity Level	• Level 3
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 organization's payment systems secure ▪ It identifies the need for monitoring and mitigating threats to the system and for incident management
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 gives 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 2.6.1
Scope and Application	See Section 2.6.1

References	http://www.iso.org/ https://www.pcisecurityStandards.org/

2.7 Workforce & Resource Management

Purpose	Framework for defining ICT Skills required in an organization.
Justification	**Business Challenge** • Difficulty in recognizing and nurturing to achieve significant productivity gains over a period of time **How this Capability Addresses this Challenge** • It provides a system for IT Professionals to match the Skills of the workforce to the requirements of the business **Business Benefits** • Improves Standard reference for recruitment, deployment and development of staff • Improves management communication by ensuring that common skills language is being used throughout the organization • Ensures a functioning organization that is focused on delivering quality outcomes • Solves critical business problem by Improving people management processes through the following: – Identification of strengths in knowledge and skills – Career pathway mapping – Identification of gaps for training plans and skills matching – Improved Performance management and succession planning
Standard	• Skills Framework for the Information Age (SFIA)
Version of the Standard to which Compliance is Required	• SFIA version 5
Minimum Acceptable Maturity Level	• Level 3 (Competency analysis, Competency Development, Workgroup Development, Career Development and Workforce Planning)
Description of Standards	• The SFIA is a model widely adopted in the United Kingdom for describing and managing competencies for ICT professionals

Rationale for Selection	**SFIA** • SFIA provides a common reference model for the identification of the skills and competencies required by ICT professionals and maps out 101 identifiable skills, categorized into 6 main areas: o Strategy and architecture o Business change o Solutions development and implementation o Service management o Procurement and management support o Client interface • The Standard is freely available for download and use
Benefits	• Improved deployment of IT skills within the organization • Improved alignment of skills to functional roles resulting in effectiveness and greater staff retention • Improved skills development and career path planning
Requirements for compliance	In order to be compliant to the industry Standard the requirements of the SFIA framework must be implemented. **Process for compliance** • Implement the SFIA framework and submit to a formal assessment by the IT Standards Council • If all requirements are met, the organization will be deemed to have complied by the IT Standards Council.
Scope	This Standard shall be applicable to all banks and external (managed) service providers in the Banking industry.

Key Elements of the Standards
SFIA: • The Standard specifies skills categories divided into six main areas with sub categories as follows: o Strategy and planning: ▪ Information strategy ▪ Advice and guidance ▪ Business/IT strategy and planning ▪ Technical strategy and planning o Business change ▪ Business change implementation ▪ Business change management ▪ Relationship management

- Solutions development and implementation
  - Systems development
  - Human factors
  - Installation and integration
- Service management
  - Service Strategy
  - Service Design
  - Service transition
  - Service Operation
- Procurement and management support
  - Supply management
  - Quality Management
  - Resource management
  - Learning and development
- Client interface
  - Sales and marketing
  - Client Support

- In addition, seven levels of responsibility are also defined:
  - Follow: Basic capability to complete tasks under close supervision. Not expected to use much initiative. Should be organized, capable of learning and contributing to own development plan.
  - Assist: Uses some discretion and has a wider circle of interaction than level 1, especially in specialty. Works on a range of tasks, and proactively manages personal development.
  - Apply: Complete work packages with milestone reviews only. Escalates problems under own discretion. Works with suppliers and customers. May have some supervisory responsibility. Performs a broad range of tasks, takes initiative, and schedules own and others work.
  - Enable: Works under general direction in a framework. Influence at account level, works on a broad range of complex activities. Good level of operational business skills.
  - Ensure and advise: Broad direction, supervisory, objective setting responsibility. Influences organization. Challenging and unpredictable work. Self-sufficient in business skills.
  - Initiate and influence: Authority for an area of work. Sets organizational objectives. Influences policy, significant part of organization, and customers and suppliers at a high level. Highly complex and strategic work. Initiates and leads technical and business change.
  - Set strategy, inspire, and mobilize: Authority includes setting policy. Makes decisions critical to organization, influences key suppliers and customers at top level. Leads on

strategy. Full range of management and leadership skills. Ref : http://www.sfia.org.uk/

3 Re-prioritised Industry IT Standards

3.1 Re-prioritised IT Standards

The IT Standards are prioritized based on **Effort** (ease of implementation of a Standard is a function of the efforts required to implement, the implementation costs as well as the duration and risks of implementation) and **Benefits** (the impact of implementation on the business and on the end user, the benefits derivable as well as the time it takes to begin deriving value from the implementation of the Standard)

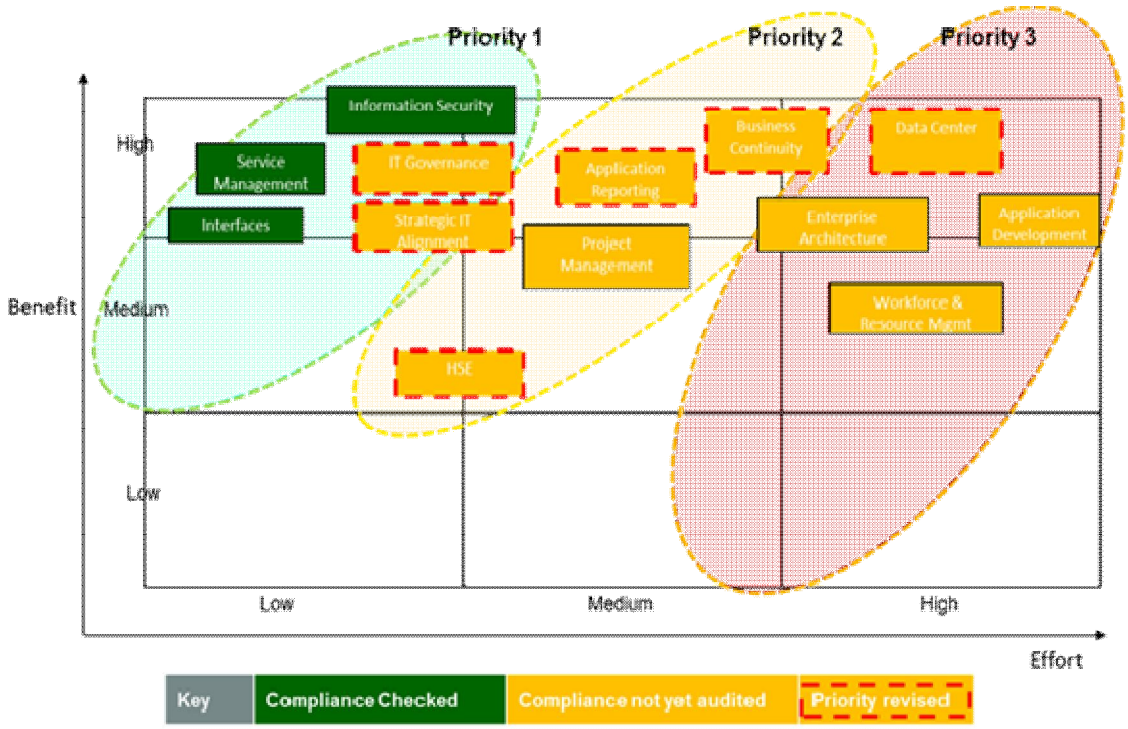

Figure 1 - IT Standards Prioritization

The IT Standards areas prioritisation is as follows:

Priority 1 Standards:

- IT Governance
- Strategic IT Alignment
- Service Management
- Interfaces
- IT Security

Priority 2 Standards

- Project Management
- Application Reporting
- Business Continuity Management
- Health, Safety and Environment

Priority 3 Standards

- Enterprise Architecture
- Application Development
- Workforce and Resource Management
- Data Centre

The Standards shall be implemented using a continuum approach such that initial implementations would target the agreed maturity level 3 and subsequently improved to include higher maturity levels if desired by the institution

3.2 **IT Standards Adoption Roadmap**

A six year roadmap for banks to adopt the following Standards at maturity level 3 is therefore proposed based on the priorities. It is recommended that formal assessment by the IT Standards Councils begin at the end of the prescribed periods.

			2014	2015	2016		2017		2018		2019	
Capability Area		Standards		Nov	June	Sept	June	Sept	June	Sept	June	Sept
Strategic IT alignment		ITIL/ COBIT										
IT Governance		COBIT/ ISO 38500										
Architecture & Information Management	Interfaces	ISO 8583 / ISO 20022										
	Reporting	XBRL										
	Enterprise Architecture	TOGAF										
Solution Delivery	Applications Development	CMMI-Dev										
	Project Management	PMBOK/ PRINCE2										
Service Management & Operations	Service Management	ITIL/ ISO20000										
	Data Center	Tier Standards - Tier 942										
	HSE	OHSAS 18001										
	Business Continuity	BCI GPG/ ISO 22301										
Information & Technology Security		PCI DSS										
		ISO 27001/27002										
Workforce & Resource Mgmt.		SFIA										

Key: Compliance checked | Compliance not checked

Figure 2: IT Standards Implementtaion and Adoption Timeline

4 Considerations for IT Service Provider/Vendor Engagement

4.1 Considerations for Engaging IT Vendors and Service Providers

Most Banking 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 Banking 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 Bank to Banking loss, regulatory action or even reputational damage.

The use of service providers does not relieve a Bank's board of directors and executive management of their responsibility to ensure that service providers' activities are conducted securely and in compliance with the Bank'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 Banking Institutions already have policies guiding interactions with contractors, vendors and service providers. This may already exist via the Bank's business policies, or through the implementation of IT Standards like ITIL, ISO 20000, COBIT and /or ISO 27001. CIOs are expected to conform to these policies where they exist and also ensure that they are aligned to Bank'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

Banking 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, Banking performance, and business continuity /contingency plans (where applicable). Banks 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 Card Processing	▪ 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 Centre	▪ Telecommunications Industry Association's Telecommunications Infrastructure Standard for Data Center - TIA-942 ▪ 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 a thorough and rigorous contracting procedures

   The contract with the vendor/service provider must be drawn up in conjunction with and reviewed by the Bank'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 Banking 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 Bank 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. Banks are encouraged to monitor vendors/service providers for compliance with contracts and service level agreements. Banks are encouraged to validate business

continuity and contingency plans for vendors /service providers who support critical business functions or provide mission critical activities

Banking 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.

5 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 Banks 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?	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 3 is required for all Banks.
4	Can a phased maturity plan be adopted by Banks to attain maturity level 3	Phased maturity plans can be adopted by Banks. However, Banks 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 Banks to implement?	Banks are required to implement only one Standard per area of IT concern. Banks 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 Banks from implementing the IT Standards.
7	Can the Banks extend the scope of new and already implemented Standards?	Banks can extend the current Standards as long as the minimum features / requirements of the Standards defined for the Industry are met
8	Are Banks with foreign affiliation required to adopt the IT Standards?	Yes. Standards defined for the local industry are expected to be adopted by every Bank irrespective of affiliation or parentage.
9	Will self-audit/assessment by a	Internal audits / checks may be performed to ensure Bank's own compliance. However only

S/N	Feedback from the Banks	Response
	Bank's internal formal assessment by the IT Standards Council sufficient?	reports from the Compliance Management Committee and Independent Assessors will be used for compliance purposes by the IT Standards Council.
10	Will there be exemptions for some Banks with regards to adopted IT Standards?	There will no exemptions. All banks will be required to implement all agreed IT Standards
11	Will partial implementation of Standards such as CMM - Dev be accepted?	No. Banks are at liberty to determine how they approach Standards implementation. However, the minimum features/ requirements of the Standards defined for the Industry as well as maturity level must be met.
12	How would new, excluded or obsolete IT Standards e.g. risk management, PA-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 Banking reporting, implementation of the IFRS taxonomy suffices for XBRL compliance. However, it does not cater to other forms of business information reporting

6 Appendix

6.1 IT Trends and the Implications for the Nigerian Banking Industry

Globally the Banking 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 and
- Mobility,

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

Successful Banking 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 Banking institutions meet customer expectations.

IT Standards covering these trends are still evolving and there no globally accepted Standards yet. What we have are guidelines localized in different countries where they exist. Guidelines for adoption of these trends for the Banking 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 Banking Industry in Nigeria.

6.1.1 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 organization 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 organization 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 bank gives away data that might be sensitive and confidential. The organization 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 organization 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 Banking to the public cloud can be enormous if not properly controlled

6.1.2 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 organizations, a powerful means to deliver deliver superior customer experience by improving their communications, processes and, ultimately, performance. The Banking industry is fully aware and is taking measures to tap into the benefits of social media.

Today, the Banking 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 Banking institutions

Implications (Positive) of Adopting Social Media

- Improves search engine optimization rankings and brand recognition: Having social media pages makes the organization look legitimate and trustworthy to search engines. The more an organization engages in social media conversation, the more likely the organization 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 organization 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 bank 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 organization 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 organization 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

6.1.3 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, Banking institutions have witnessed a steady acceleration and expansion in Technology outsourcing. It represents an opportunity for Banking firms 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 Banking 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, Banking conditions, and technologies all change very quickly. Outsourcing providers assume and manage much of these risks for the organization 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 organization 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 organizations at a time. In such situations vendors may lack complete focus of the organization’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 organization 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 exist, but 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.

6.1.4 **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. Banks 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 banks achieve three critical objectives for banking transformation:

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

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

Big data capabilities provides banks 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 banks 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 Banking 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 banks 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

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

Mobility fosters Banking inclusion by helping underserved consumer's access safe, convenient, and affordable Banking by encouraging more Banking-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 organization 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 Banking 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