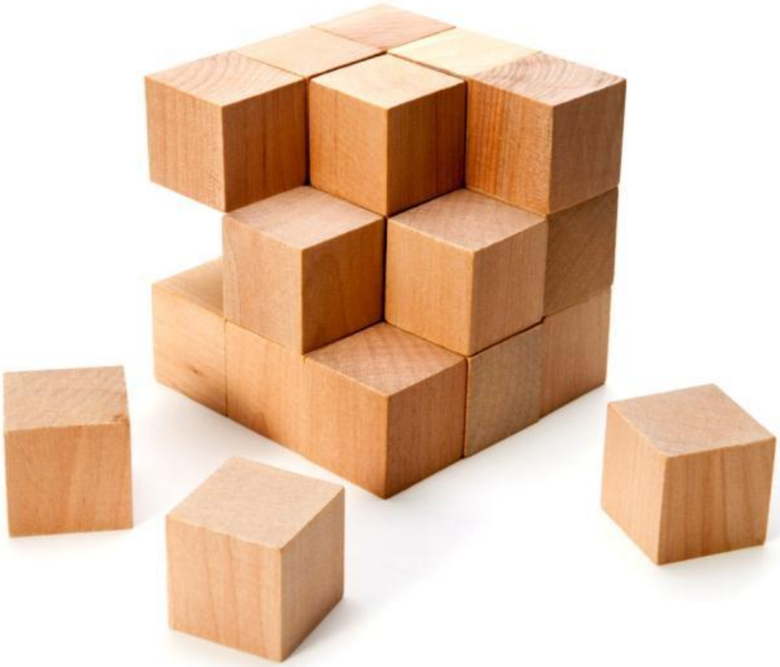
Digital Jewels

Q1 2015 IVC BREAKFAST FORUM



Demystifying the CBN IT Standards Blueprint

CHIDI UMEANO
HEAD, SHARED SERVICES
CBN

Background & Objectives

- ❑ Information Technology has fundamentally transformed the business architecture of banks resulting in evolution of new business architectures and approaches to customer service, enterprise management and regulatory compliance.

- ❑ IT spend in the Nigerian financial services industry as a proportion of overall operating expenses is high and increasing, however, commensurate value is not realised from the investments. Some of the existing issues include:
  - Complex, duplicate, non-standard and costly processes
  - Non-standard systems and infrastructure
  - Inefficiency of electronic information exchange
  - Data integrity issues

- ❑ Industry leverage of IT lags global leading practices and is limiting banking operating efficiency, cost effectiveness, regulatory information and risk management practices.

- ❑ To address this gap and provide guidelines for application and utilisation of Information Technology, Industry IT Standards were defined to articulate and provide a point of reference for the utilisation of IT

Background & Objectives
- Issues

Prior to the drive by CBN on IT standards, there were no defined IT Standards driving interoperability, information exchange, enterprise architecture, and system integration amongst others in the industry with implications such as:

- ❑ High cost of integration as banks' IT Infrastructure cannot interact with each other or other third parties such as NIBSS, SWIFT, Interswitch e.t.c without the implementation of dedicated interfaces. Thus banks are forced to maintain different interfaces to different service providers thereby increasing cost of service.
- ❑ Interoperability and automation to drive straight through processing cannot be achieved leading to islands of automation but no integration.
- ❑ Quality and maturity of IT cannot be ascertained having no reference point to benchmark against.
- ❑ Poor customer experience in use of bank's IT infrastructure due to absence of a minimum IT standards driving governance, service management, and infrastructure
- ❑ Ad hoc implementation of CBN / regulatory policies and plans around IT (i.e. FSS2020

Background & Objectives
- Benefits of IT Standards to the Industry

- 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

Some Case Studies

Nigeria is not the only country, where the Central Bank has had to enforce or drive certain IT Standards within their local industry.

Country	Regulation	Authority	Summary
Australia	APS 232	Australian Prudential Regulatory Authority (APRA)	APRA regulation for BCM in financial services firm
Bahamas	PU 19-0406 Supervisory and Regulatory Guidelines for BCM	The Central Bank of Bahamas	Apply to all commercial banks operating in the Bahamas, based upon Basel II
Brazil	NBR 15999-1 and NBR ISO/IEC 24672	ABNT	Straight translation of the BS 25999 and ISO 24672 standards
China	a) HKMA BCP supervisory policy TM-G-2 b) IT Security Guidelines	a) Hong Kong Monetary Authority (HKMA) b) IT Services Dept. – The Government of Hong Kong Special Admin region	a) supervisory policies, minimum standards authorised institutions are expected to attain b) general concepts relating to IT Security
Croatia	a) Act on Credit Institutions b) Rules on adequate governance of IT	Croatian National Bank (CNB)	Set up a minimum control measures for proper IT Governance in banks and financial institutions. External and internal IS auditing mandated, reports provided to CNB.
Malaysia	BNM/RH/GLO13-3 Guidelines on Management of IT	Central Bank of Malaysia	Enforces minimum BCM requirements, auditing mandatory
UK	BC Practice Guide BS 25999-1:2006 BS 25999-2:2007 BS 25777:2008 IT Service Continuity	FSA (Finance Services Auth.) Bank of England British Standards Institution	Guidance on BCM req. FSA based its BCM inspection on 7 Basel Forum principles

IT Capability Areas

❑ IT standards for Nigeria's Financial Services Industry focuses on 7 key areas which are required for world class IT operations as follows:

1	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.
2	IT Governance	Framework for initiation, endorsement, sponsorship, approval and evaluation of IT decisions.
3	Architecture & Information Management	Guidance for the creation and execution of the strategic IT architecture framework.
4	Solutions Delivery	Framework for the development of software application solutions and their subsequent transition into the production environment.
5	Service Management & Operations	Planning, delivery and measurement of day-to-day operational service.
6	Information & Technology Security	Security and protection of enterprise information and related assets.
7	Workforce & Resource Management	Management of IT skills, knowledge and financial resources.

Adopted IT Standards Summary

❑ In 2010 the following standards were agreed by the CIOs for the industry across 7 IT Capability areas.

Capability		Reference	
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 (CMMI)	ISO 15504
	Project Management	Project Management Body of Knowledge (PMBOK)	PRojects IN Controlled Environments version 2 (PRINCE2)
Service Management & Operations	Service Management	ITIL	ISO 20000
	Data Centre	Tier Standards	TIA 942
	Health, Safety, Environment (HSE)	OHSAS 18001	
	Business Continuity	Business Continuity Institute Good Practice Guidelines (BCI GPG)	BS25999 / ISO 22301 (BS25999 is obsolete and superseded by ISO 22301)
Information & Technology Security	Payment Card Security	Payment Card Industry Data Security Standard (PCI DSS)	
	Information Security	ISO 27001/27002	
Workforce & Resource Management		Skills Framework for the Information Age (SFIA)	

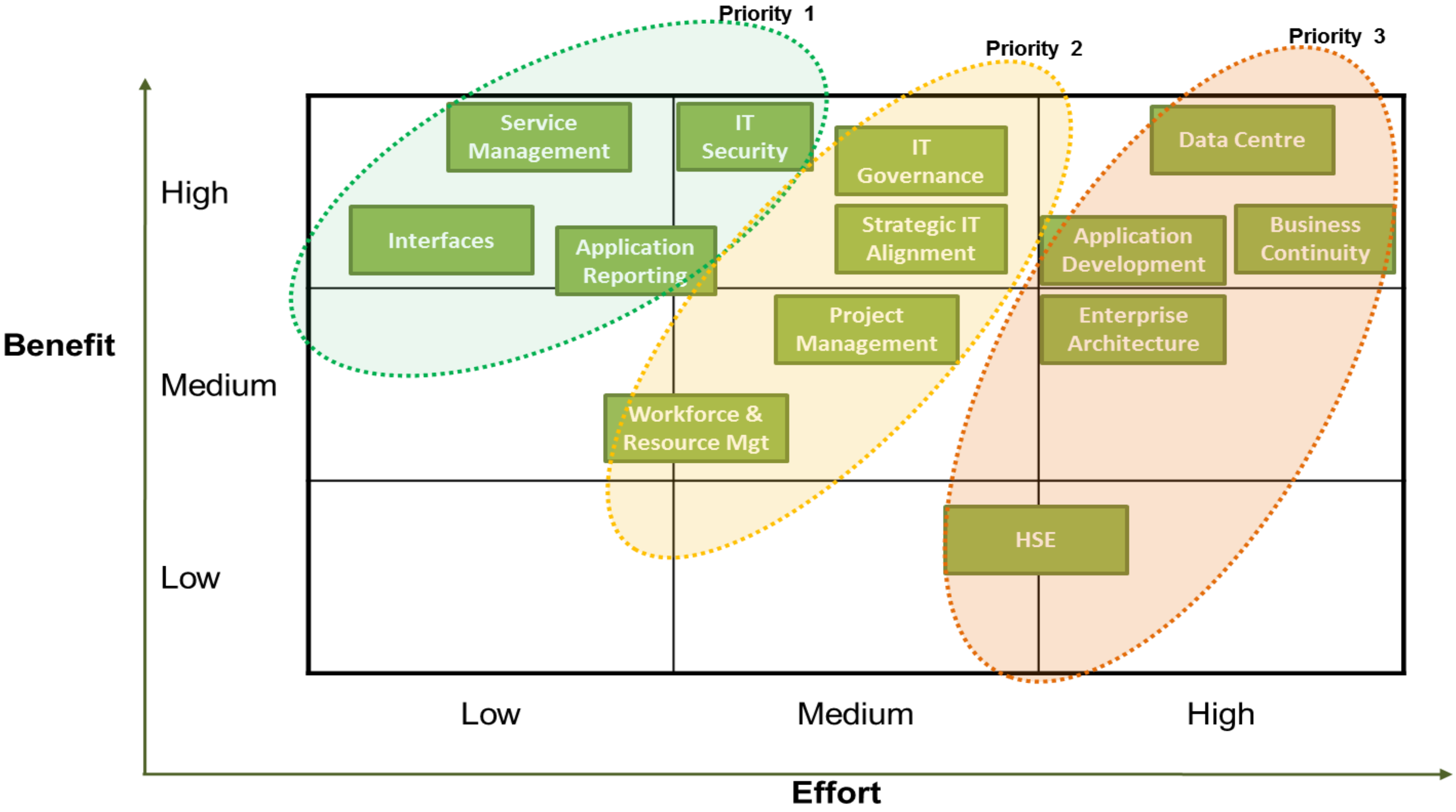
Adopted Maturity Level for Banks’ IT

❑ A maturity level of 3 is base IT maturity level for the IT standards for Nigeria’s FS Industry

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

Standards Prioritisation

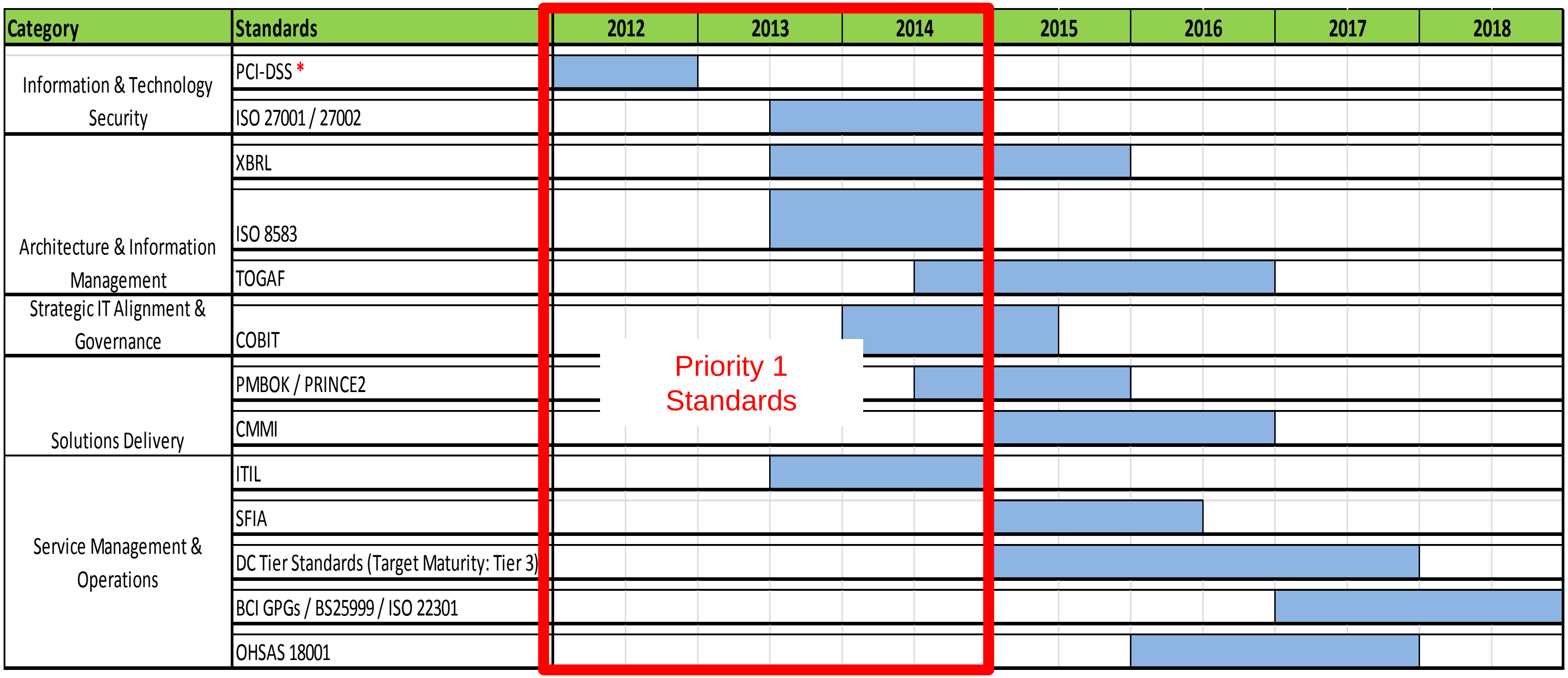
- ❑ The standards were prioritised based on efforts required for implementation as well as benefits derivable.



Current Industry IT Standards Roadmap

- A five year roadmap had been defined for banks to adopt the following standards at maturity level 3 or its equivalent. Current focus of the IT Standards Council is to ensure compliance to priority 1 standards

- This approach ensures that the Banks do not have to implement all the IT Standards at once but through phases that will be monitored by the Council.



Category	Standards	2012		2013		2014		2015		2016		2017		2018	
Information & Technology Security	PCI-DSS *	■	■												
	ISO 27001 / 27002				■	■	■								
Architecture & Information Management	XBRL				■	■	■	■	■						
	ISO 8583				■	■	■								
	TOGAF						■	■	■	■	■				
Strategic IT Alignment & Governance	COBIT					■	■	■							
Solutions Delivery	PMBOK / PRINCE2						■	■	■						
	CMMI							■	■	■	■				
Service Management & Operations	ITIL				■	■	■								
	SFIA							■	■	■					
	DC Tier Standards (Target Maturity: Tier 3)							■	■	■	■	■	■		
	BCI GPGs / BS25999 / ISO 22301											■	■	■	■
	OHSAS 18001									■	■	■	■		

IT Standards Council Brief Overview (1/2)

- ❑ The IT Standards Council was inaugurated on the 10th of May, 2013 by the Deputy Governor of Central Bank; Tunde Lemo with the mandate to drive the adoption, implementation and compliance to Industry IT standards in the Nigerian Financial Services Industry

- ❑ IT Standards Council is chaired by a Bank representative and comprises of 8 Banks and 3 CBN departments namely: IT, Shared services and Banking supervision departments.

- ❑ The Terms of Reference (ToR) of the IT Standards Council are:
  - – Promote IT Standards for Nigeria's Financial Services Industry
  - – Set strategic direction on IT Standards for the Industry.
  - – Determine the IT Standards to be implemented across the Industry.
  - – Review and update of Industry IT Standards
  - – Monitor compliance to IT Standards and determine response for deviations

IT Standards Council Brief Overview (2/2)

❑ Based on its mandate, the IT Standards Council carries out 2 major activities on a periodic basis (annually) amongst other things. They include:

S/N	Activity	Description
1	IT Standards Review	The IT Standards Council is expected to review the IT Standards annually to ensure that the IT Standards are still relevant to the industry. During these reviews; changes to standards i.e. version changes; new standards and standards to be dropped are considered by the IT Standards Review committee and recommendations are passed to the Council for ratification and implementation. **The next IT Standards Review will start in January 2015**
2	IT Standards Compliance Assessment / Audit	On an annual basis the level of compliance of Banks to the Standards defined are assessed or audited. This is to ensure that the state of the Industry with respect to the standards are known and progress can be tracked. Due to the significant number of standards under consideration, a 5 year roadmap has been defined to enable banks implement these standards in phases. Also the standards have been prioritized taking into consideration the ease of implementation and benefit to the Banks and Industry at large. This implies that not all the standards will be assessed or audited at a time. **Compliance audit was carried out for PCI-DSS in December 2013. The next IT Standards Compliance Assessment / Audit is the baseline assessment to kick off last week of February and will focus on 3 priority 1 standards namely ISO 27001, ITIL, and ISO 8583**

Strategic IT Alignment
- ITIL

IT Infrastructure Library (ITIL)	
Description	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. Current version of ITIL is version 2011.
Purpose	ITIL 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. The core publications are • Service Strategy • Service Design • Service Transition • Service Operation • Continual Service Improvement
Certification Body	ITIL Certification Management Board (ICMB)
Rating Criteria	Maturity Level 3

Strategic IT Alignment
- COBIT

Control Objectives for Information and related Technologies (COBIT)	
Description	COBIT is a Framework that 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. Adopted COBIT version is COBIT 4.1, however, current version of COBIT is version 5
Purpose	COBIT defines IT activities in a generic process model within four domains: • Plan and Organize: Strategy and tactics, and concerns the identification of the way IT contributes to the achievement of business objectives. • Acquire and Implement: To realize the IT strategy, IT solutions must be identified, developed or acquired, implemented and integrated into business processes. • Deliver and Support:Actual delivery of IT services, including IT service delivery, IT security and continuity, service support for users, and management of data and operational facilities • Monitor and Evaluate: All IT processes shall be regularly assessed over time for quality and compliance with control requirements The domains map to the IT function’s traditional responsibility areas of plan, build, run and monitor.
Certification Body	ISACA
Rating Criteria	Maturity Level 3

IT Governance
- COBIT

Control Objectives for Information and related Technologies (COBIT)	
Description	COBIT is a Framework that 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. Adopted COBIT version is COBIT 4.1, however, current version of COBIT is version 5
Purpose	COBIT defines IT activities in a generic process model within four domains: • Plan and Organize: Strategy and tactics, and concerns the identification of the way IT contributes to the achievement of business objectives. • Acquire and Implement: To realize the IT strategy, IT solutions must be identified, developed or acquired, implemented and integrated into business processes. • Deliver and Support:Actual delivery of IT services, including IT service delivery, IT security and continuity, service support for users, and management of data and operational facilities • Monitor and Evaluate: All IT processes shall be regularly assessed over time for quality and compliance with control requirements The domains map to the IT function's traditional responsibility areas of plan, build, run and monitor.
Certification Body	ISACA
Rating Criteria	Maturity Level 3

IT Governance
- ISO38500

ISO 38500	
Description	The ISO/IEC 38500 standard is a framework that provides for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations' use of IT. The standard specifies the minimum requirements for the IT Governance of an organization.
Purpose	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. ISO 38500 draws upon a number of sources, the main one being AS 8015:2005, which defines six principles for good corporate governance of IT Responsibility, Strategy, Acquisition, Performance, Conformance and Human Behaviour.
Certification Body	ISO is not involved in the certification to any of the standards it develops. Certification is performed by external certification bodies, which are largely private.
Rating Criteria	Maturity Level 3

Architecture and Information Management (Interfaces) - ISO 8583

ISO 8583	
Description	ISO 8583 also known as Financial Transaction Card Originated Messages – Interchange Message Specifications, provides a standard framework for systems that exchange electronic transactions made using payment cards
Purpose	It is a common interface by which financial 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 value 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 Most core Banking application vendors provide native ISO 8583 interfaces and ISO 8583 is widely adopted within the Nigerian Financial Services industry for card based payment transactions.
Certification Body	ISO is not involved in the certification to any of the standards it develops. Certification is performed by external certification bodies, which are largely private.
Rating Criteria	All organizations that provide payments services are required to provide ISO 8583 compliant interfaces

Architecture and Information Management (Interfaces) - ISO 20022

ISO 20022	
Description	Also known as the Universal financial industry (UNIFI) message scheme provides a common platform for the development of messages in a standardized XML syntax and is the de-facto standard adopted in Europe to facilitate the Single Euro Payments Area (SEPA).
Purpose	It provides communication interoperability between financial institutions, market infrastructure and end-users in respect of financial 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
Certification Body	ISO is not involved in the certification to any of the standards it develops. Certification is performed by external certification bodies, which are largely private.
Rating Criteria	Compliance with ISO 20022 requirements is currently not mandatory

Architecture and Information Management (Reporting) - XBRL

eXtensible Business Reporting Language (XBRL)	
Description	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. The current (2008) version of XBRL is 2.1, with errata corrections.
Purpose	XBRL provides a method to prepare, publish, exchange, search and analyze financial statements across all software formats and technologies. It includes an IFRS taxonomy which facilitates the electronic use and exchange of financial data in line with IFRS directives. 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 • 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
Certification Body	XBRL International manages XBRL certification
Rating Criteria	Implement XBRL and submit to a compliance audit If all requirements are met, the organization will be deemed to have complied by the IT Standards Governance Council

Architecture and Information Management (Enterprise Architecture) - TOGAF

The Open Group Architecture Framework (TOGAF)	
Description	The TOGAF Architecture Development Method (ADM) is a framework for developing an enterprise architecture covering Business Architecture, Application Architecture, Information Architecture and Technology Architecture. Current version is version 9
Purpose	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, Information Systems Architecture, Technology Architecture, Opportunities and Solutions, Migration Planning, Implementation Governance and Architecture Change Management are the remaining phases
Certification Body	The Open Group manages the TOGAF certification
Rating Criteria	Maturity Level 3

Solutions Delivery (Applications Development) - CMM

Capability Maturity Model Integration (CMMI)	
Description	The CMMI is a Framework for projects or organizations that provides common, integrated, and improving processes for Systems and Software development.
Purpose	It provides a set of best practices that address productivity, performance, costs, and stakeholder satisfaction and can be utilized to drive significant value realization. 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 Detailed Processes of the Capability Maturity Model Integration (CMMI) can be seen in the slide "Adopted Maturity Level for Banks' IT"
Certification Body	CMMI Institute manages the CMMI certification
Rating Criteria	Maturity level 3

Solutions Delivery (Applications Development) - ISO 15504

ISO 15504	
Description	ISO 15504 is a framework for process assessment which defines processes and a capability dimension for measuring the processes
Purpose	ISO 15504 contains a reference model which defines processes and a capability dimension for measuring the processes. The process dimension defines processes divided into the six process categories of: • Processes • Customer supplier • Engineering • Supporting • Management • Organization Capability levels include • 5 - Optimizing Process • 4 - Predictable Process • 3 - Established Process • 2 - Managed Process • 1 - Performed Process • 0 - Incomplete Process
Certification Body	ISO is not involved in the certification to any of the standards it develops. Certification is performed by external certification bodies, which are largely private.
Rating Criteria	• Implement the requirements of the ISO 15504 standard • Submit to a compliance audit by a certified assessor. • Provide the results to the IT Standards Governance Council as proof of compliance

Solutions Delivery (Project Management) - PMBOK

Project Management Body of Knowledge (PMBOK)

Description	The PMBOK is a global standard which establishes best practices and principles for project management.
Purpose	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
Certification Body	Project Management Institute (PMI) manages the PMBOK certification.
Rating Criteria	Maturity Level 3

Solutions Delivery (Project Management) - PRINCE2

PRojects IN Controlled Environments version 2 (PRINCE2)

Description	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
Purpose	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 • Initiating a project: This process builds on the work of the startup process, and the project brief is augmented to form a Business case. • Directing a project: This process dictates how the project board should control the overall project. • 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. • Managing stage boundaries: This dictates what should be done towards the end of a stage. • 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.
Certification Body	APMG International
Rating Criteria	Maturity Level 3

Service Management & Operations (Service Management) - ITIL

IT Infrastructure Library (ITIL)	
Description	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. Current version of ITIL is version 2011.
Purpose	ITIL 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. The core publications are • Service Strategy • Service Design • Service Transition • Service Operation • Continual Service Improvement
Certification Body	ITIL Certification Management Board (ICMB)
Rating Criteria	Maturity Level 3

Service Management & Operations (Service Management) - ISO 20000

ISO 20000	
Description	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. The ISO 20000 standard specifies a set of inter-related management processes and is derived from ITIL.
Purpose	The Standard promotes an integrated service management model comprising of the following: • Requirements for a Management System • Planning and Implementing Service Management • Planning and Implementing new or changed services • Service Delivery Processes • Relationship Processes • Resolution Processes • Control Processes • Release Processes
Certification Body	ISO is not involved in the certification to any of the standards it develops. Certification is performed by external certification bodies, which are largely private.
Rating Criteria	• 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 Governance Council as proof of compliance

Service Management & Operations (Data Centre) - TIER STANDARDS (UPTIME)

Tier Standards	
Description	The Tier Standard establishes four distinctive definitions of data centre site infrastructure Tier classifications (Tier I, Tier II, Tier III, Tier IV), and the performance confirmation tests for determining compliance to the definitions.
Purpose	The Tier classifications describe the site-level infrastructure topology required to sustain data centre operations, not the characteristics of individual systems or subsystems. The Tiers are as follows • Tier I - Basic Site Infrastructure • Tier II - Redundant Site Infrastructure Capacity Components • Tier III - Concurrently Maintainable Site Infrastructure • Tier IV - Fault Tolerant Site Infrastructure
Certification Body	The Uptime Institute
Rating Criteria	• Upgrade data centre to meet Tier 3 requirements. • Notify the IT Standards Governance Council of compliance audit readiness • Submit to compliance audit • If all requirements are met, the organization will be deemed to have complied by the IT Standards Governance Council

Service Management & Operations (Data Centre) - TIA 942

TIA 942	
Description	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
Purpose	The standard is primarily a telecom infrastructure standard, but also addresses data centre facility requirements as follows: • Site space and layout • Cabling infrastructure • Tiered reliability • Environmental considerations
Certification Body	TIA
Rating Criteria	• Submit to compliance audit • The audit will provide a report of non-compliances as well as a "EPI Certificate" indicating the level of compliance to the ANSI/TIA-942 standard. • In the following two subsequent years the Data Centre will need to go through a surveillance audit. In the third year a complete (re)certification audit will be conducted to re-establish the Tier classification

Service Management & Operations (Health, Safety, Environment (HSE)) - OHSAS 18001

OHSAS 18001	
Description	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
Purpose	• 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. The key elements of the Standard are • Planning • Implementation and Operation • Checking and Corrective Action • Management review
Certification Body	BSI Group
Rating Criteria	• Implement a Health and Safety Management System to meet the requirements of the OHSAS standard • Submit to a compliance audit by OHSAS auditors. • Provide a certificate of compliance to the IT Standards Governance Council as proof of compliance

Service Management & Operations (Business Continuity) - BCI GPG

Business Continuity Institute Good Practice Guidelines (BCI GPG)

Description	The BCI GPG is a holistic set of guidelines developed by the Business Continuity Institute which specifies the Professional Practices that cover all the phases of a Business Continuity Management Lifecycle
Purpose	• 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. The key elements of the Standard are • Planning • Implementation and Operation • Checking and Corrective Action • Management review
Certification Body	Business Continuity Institute
Rating Criteria	• Implement the requirements of the BCI GPG and submit to a compliance audit • If all requirements are met, the organization will be deemed to have complied by the IT Standards Governance Council

Service Management & Operations (Business Continuity) - BS 25999 (ISO22301)

BS 25999 (ISO22301)

Definition	Business Continuity Management standard that applies Business Continuity Planning to enterprises. BS 25999 is in 2 parts; BS 25999-1 and BS 25999-2 . In December 2012, the BS25999 standard was retired and replaced with the ISO 22301
Purpose	BS 25999-1 establishes processes, principles and terminology for Business Continuity Management. It covers the following key areas: • The Business Continuity Management Policy • BCM Programme Management • Understanding the organization • Determining BCM Strategies • Developing and implementing a BCM response • Exercising, maintenance, audit and self-assessment of the BCM culture • Embedding BCM into the organizations culture BS 25999-2 (ISO22301) • Planning the Business Continuity Management System (PLAN • Implementing and Operating the BCMS (DO). • Monitoring and Reviewing the BCMS (CHECK)
Certification Body	BSI Group
Rating Criteria	• Implement the controls specified in the specification section of the standard • Request an assessment from an accredited BS 25999 (ISO22301) auditor • Provide the results to the IT Standards Governance Council as proof of compliance

Information & Technology Security (Payment Card Security) - PCI-DSS

Payment Card Industry Data Security Standard (PCI DSS)

Description	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
Purpose	• Build and Maintain a Secure Network • Protect Cardholder Data • Maintain a Vulnerability Management Program • Implement Strong Access Control Measures • Regularly Monitor and Test Networks • Maintain an Information Security Policy
Certification Body	PCI Security Standards Council
Rating Criteria	• Implement required controls • Engage a QSA to conduct a compliance audit • Provide the results to the IT Standards Governance Council as proof of compliance

Information & Technology Security (Information Security) - ISO 27001/27002

ISO 27001/27002	
Description	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
Purpose	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
Certification Body	ISO is not involved in the certification to any of the standards it develops. Certification is performed by external certification bodies, which are largely private.
Rating Criteria	• Implement the requirements of the ISO 27001 standard • Submit an application for assessment to an accredited certification body to conduct the compliance audit.

Workforce & Resource Management - SFIA

Skills Framework for the Information Age (SFIA)	
Description	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: • Strategy and architecture • Business change • Solutions development and implementation • Service management • Procurement and management support • Client interface
Purpose	• Strategy and planning: • Business change • Solutions development and implementation • Service management • Procurement and management support • Client interface
Certification Body	SFIA Foundation
Rating Criteria	• Implement the SFIA framework and submit to a compliance audit • If all requirements are met, the organization will be deemed to have complied by the IT Standards Governance Council.

Achievements till Date

❑ Definition of industry IT Standards Blueprint

❑ Setup of the IT Standards Council to drive and oversee the adoption of IT Standards within the Banking Industry

❑ Launch of IT Standards through the issuance of CBN circular to the Banks and publishing of the IT Standards on CBN website

❑ Conduct baseline assessment to determine readiness status of bank (Compliance assessment has been done for PCI DSS while that of the other 3 standards (ITIL, ISO 27001 & ISO 8583 will be done in the First half of 2014)

Next Steps

❑ Conduct review of Industry IT Standards (2015)

Link to IT Standards Blueprint

http://www.cenbank.org/ITStandards/