NIGERIAN GOVERNMENT ENTERPRISE ARCHITECTURE (NGEA)

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA)

MARCH, 2019

Change History

S/N	Author	Version No	Release Date	Change Details
1.	NITDA	1.0	March, 2019	First Review

Metadata of the Regulation

S/N	Data Elements	Values
1.	**Title**	Nigerian Government Enterprise Architecture
	Title Alternative	NGEA
2.	**Document Identifier**	NIG-NITDA.11
3.	**Document Version, month, year of release**	Version 1.0; March, 2019
4.	**Publisher**	National Information Technology Development Agency (NITDA)
5.	**Type of Regulation Document** *(Standard/ Policy/ Technical Specification/ Best Practice /Guideline / Framework /Policy Framework/Procedure)*	Framework
6.	Enforcement Category *(Mandatory/Recommended)*	Recommended
7.	Owner of approved regulation	NITDA
8.	Target Audience	All Public Institutions (including Local, State and Federal Government); ICT Product/Service Providers for public institutions; Professional Bodies; Development Partners; and General Public.
9.	Copyrights	NITDA
10.	Format *(PDF/A at the time of release of final Regulation)*	PDF
11.	Subject *(Major area of Standardization)*	Enterprise Architecture

Table of Contents

List of Figures

List of Tables

Definitions:

Information Technologies refer to the use of computing technologies such as networking, hardware, software, the Internet etc. to create, process, store, secure and exchange all forms of electronic data for the providing service(s).

IT/ICT Systems mean material computers systems, servers, network and communication equipment, software, applications, government data and other IT infrastructure owned and used by Public Institutions and that are used in the business of Nigerian Government for information processing.

e**-Government** is the use and application of information technologies in government activities to streamline and integrate workflows and processes for the purpose of effectively managing data and information, enhancing public service delivery, as well as expanding communication channels for engagement and empowerment of people.

Government Digital Capability comprises of public institutions' business process, IT systems (infrastructure, government data and core applications), e-Services applications attributed to Nigerian Government to deliver public service.

Reference Model is an abstract framework or domain-specific ontology consisting of an interlinked set of clearly defined concepts produced by an expert or body of experts in the field of Enterprise Architecture in order to encourage clear communication while defining and using IT systems.

Whole-of-Government (WoG) denotes public institutions working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues through the use of ICT.

Government Digital Transformation (GDT) denotes advanced WoG. It means Nigerian Government transformation that is ICT-enabled for the purpose of citizen-driven service delivery and empowerment; transparent and efficient government with ultimate goal of a sustainable national economic, political and social transformation.

Public Institutions means Ministries, Departments, Extra-Ministerial Departments and Agencies of Government at Federal, State and Area Council levels.

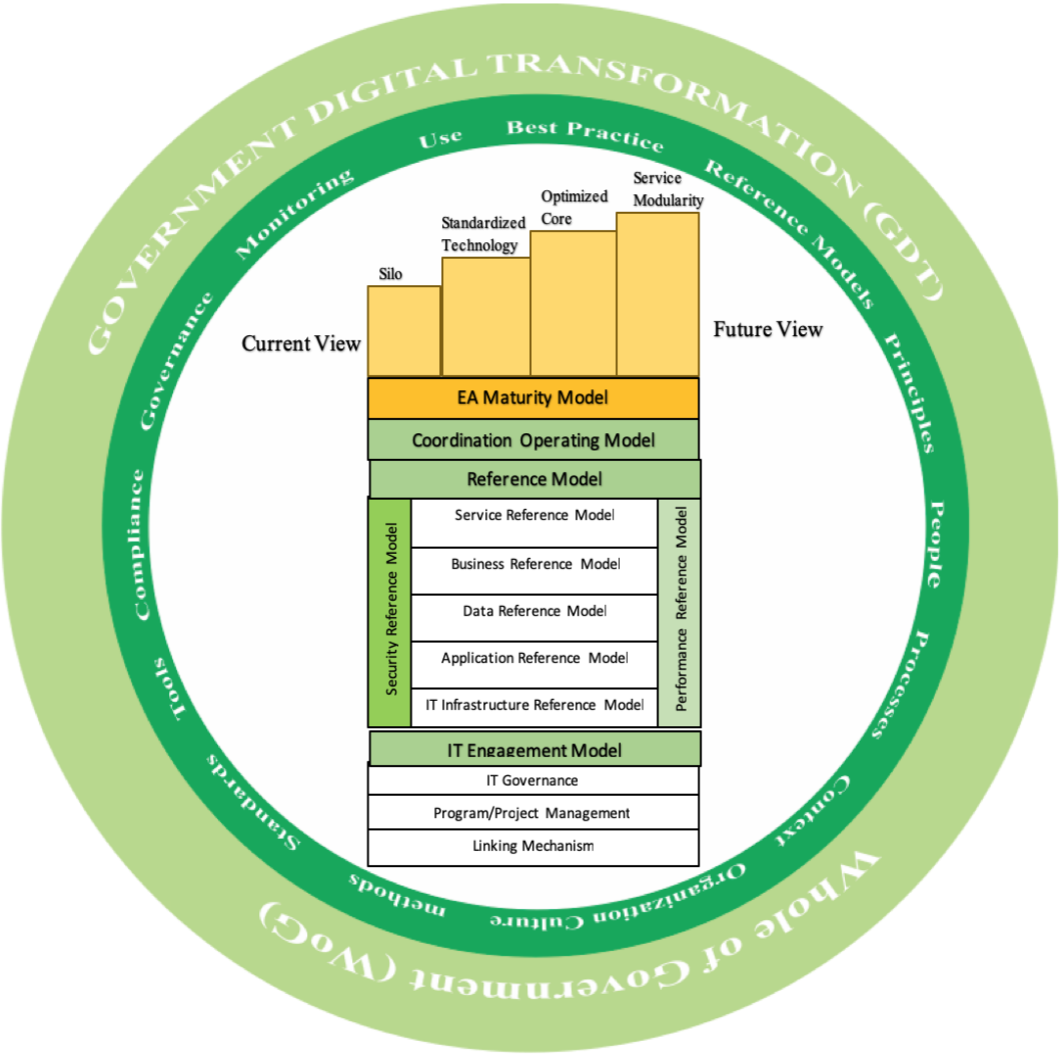
Government Enterprise Architecture is a conceptual Blueprint and Framework for efficiently re-architecting and aligning structure and operation (Nigerian Government's Processes, Information, People and other enterprise driving factors with Information Technology for the purpose of achieving Government Digital Transformation Agenda.

Acronym

FEAF	Federal Enterprise Architecture Framework

TOGAF	The Open Group Architecture Framework
Ne-GIF	Nigerian e-Government Interoperability Framework

NIGERIAN GOVERNMENT ENTERPRISE ARCHITECTURE (NGEA) AT A GLANCE



SECTION ONE: Introduction to Nigerian Government Enterprise Architecture

1.1 Background

Enterprise Architecture (EA) has been identified as a key enterprise and technology best practice that enables organizations to evolve and translate their capabilities while using Information Technology (IT) in a structured and disciplined manner into effective enterprise change. The Government of any country is a big and critical enterprise that must be managed efficiently to ensure its resources including IT are maximized to create value for stakeholders given the political, legal, managerial/administrative contexts it finds itself at any time.

One of the strategic directions for e-government across the world is adoption of a Whole-of-Government (WoG) approach. WoG connotes deviation from structural devolution, disaggregation and single-purpose organizations to more integrated approach to public service delivery. It is a paradigm shift for governments all over the world toward a vision of a connected, networked, citizen-centered government leading to Government Digital Transformation (DGT). Citizen-centered service delivery involves breaking up silos, integrating across agencies, innovating new ways of doing business, and creating a service-focused culture. Most of the developed Nations and top ranked countries in the e-Government Development Index (EGDI) have their national enterprise architectures as overarching documents that guide adoption of IT in government. Therefore, there is need for a workable and implementable framework or blueprint that articulate how WoG and GDT can be achieved in Nigeria. Governments are adopting the Enterprise Architecture concepts all over the world to effectively align government businesses and IT such that IT becomes a strategic tool for governance transformation.

1.2 What is Enterprise Architecture (EA)?

The enterprise architecture is a disciplined way of organizing enterprise resources (business processes, data, information technologies, human, finance etc.) to provide capabilities that enable the achievement of desired organizations' functions/mandates outcomes. It specifies the principles, practices, standards and policies that guide the way capabilities are evolved over time and continue to deliver results (efficient service delivery) even under a continuous change of political, administrative, economic etc. conditions. It provides an integrated and long-term view of the enterprise's strategic goals, structure, people, finance, data/information, business processes across all lines of businesses/mandates, functions and services and their relationship with information technology and the external environment with the aim of deriving maximum benefits from the use and adoption of IT in government.

EA is a framework that provides a road map for all Public Institutions to optimize their operations while creating an efficient IT environment capable of translating national or their organization's vision, policies, programs, plans, strategies into effective enterprise change and public value. It is a framework for positioning IT as a strategic asset, shaping current and future strategic opportunities in the public sector and the Government at large. In addition, it is a decision-making and management framework that enables public institutions to collaboratively provide seamless services to its citizens while providing mechanisms to maximally and continuously leveraging existing and future ICT investments in support of the Government Digital Transformation (GDT) vision.

Nigerian Government Enterprise Architecture (NGEA) is therefore is a long-term strategy and a road map for restructuring government processes, organizing government information, and deploying IT efficiently in the public sector with the goal of achieving Whole-of-Government for effective public service delivery and attainment of Government Digital Transformation in Nigeria.

1.3 The Challenge and Why Enterprise Architecture?

Public Institutions (PIs) have their respective and varied mandates. Achieving a Whole-of-Government and Government Digital Transformation calls for a shift in the way e-Government and IT systems are being deployed in Public Institutions. It is evident that our e-Government systems and IT deployments as a country are still silo-based. This is because each Public Institution is good at deploying IT systems for each of its strategic initiative and specific service without a recourse to a national long-term IT plan that follows and ensures a pre-determined process for IT systems interoperability and information exchange across Public Institutions.

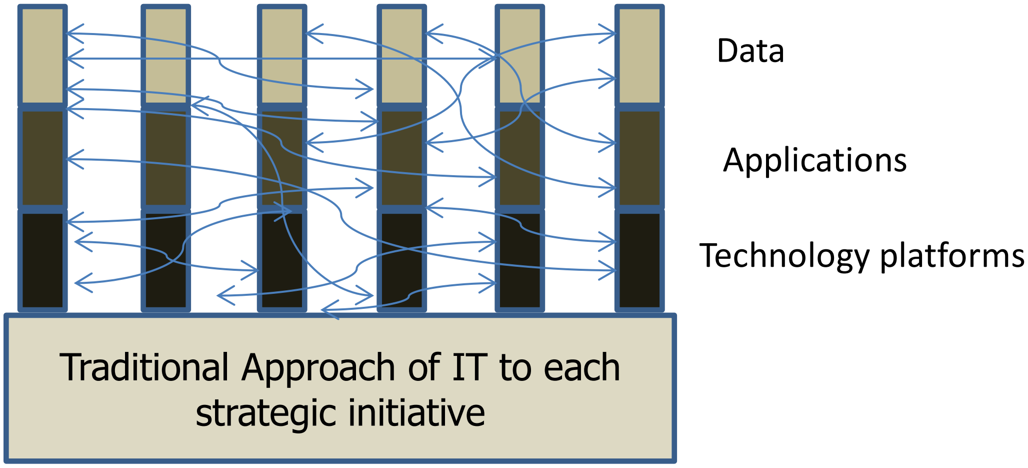


Figure 1.0: The challenge of traditional IT approach to strategic initiatives

The figure 1.0 presents the bottlenecks experienced when there is no discipline for IT deployment. All the wobbly lines are results of the efforts to integrate IT systems that are not interoperable. This makes IT a bottleneck instead of a strategic tool for transformation.

Even though IT projects/systems of some Federal Public Institutions (FPIs) have significantly advanced individually, experience has shown that as each FPI increases its IT investments and widens the scope of e-government services, IT systems are getting more complex and many problems are beginning to emerge. For instance, the following challenges are currently being experienced:

1. Inefficient and un-scalable IT environment;
2. Poor interoperability of IT systems and inability to effectively share IT resources;
3. Poor government-wide information sharing and exchange for effective service delivery;
4. Maintenance of unnecessary multiple & unstandardized communication channels, customer interfaces and applications;
5. Replication of IT resources due to inadequate knowledge of available IT resources and capabilities across the government; and
6. High cost of IT investments and poor sustainability of IT projects.
7. Inability to efficiently and effectively achieve statutory mandates.

The effect of these is inability of public institutions to fully translate national or their vision, policies, programs, plans, strategies into effective enterprise change and public value which has prevented IT, to some extent, from becoming an asset shaping strategic future opportunities of the Nigerian Government. The consequence of all these is high rate of IT projects failures.

All these have called for an efficient deployment of IT in government as it remains a strategic tool for implementing government policies, strategies, plans and programs. FPIs can leverage efficient IT systems to improve governance and create innovative solutions that will change the society.

It is on that note that National Information Technology Development Agency (NITDA), as the prime Agency for IT policy making and implementation in the country, has come up with a framework called "**Nigerian Government Enterprise Architecture (NGEA)**" to address these challenges and provide a clear road map for a WoG and GDT in Nigeria. Therefore, Nigerian Government Enterprise Architecture (NGEA) as a framework for long-term IT strategy/plan and a road map for achieving Whole-of-Government and Government Digital Transformation is apt and becomes absolutely unavoidable.

1.4 Objectives of NGEA

The main objective of NGEA is to correct all the anomalies in government processes, information management, and deployment/implementation of ICT projects across the government in the next five to ten years. Therefore, NGEA is aimed to:

1. Provide strategic choice on how IT should be deployed to ensure certain levels of standardization and integration are achieved for supporting both WoG agenda and autonomy of public institutions' mandates;
2. Provide abstract reference models at each layer of the enterprise architecture with prescription of appropriate tools, specifications, standards, requirements, best practices, methods etc. to guide IT deployment in the public sector;
3. Provide framework that ensure IT projects are scalable, shared, efficient and local content driven; and
4. Provide and devise a clear IT engagement model with appropriate structure for effective IT governance, program/project management and coordinating mechanisms that guarantee desirable behavious from IT and

ensure expected values are derived as each IT project is implemented and added to the enterprise (public sector).

5. Provide framework and abstract models for public institutions/MDAs to develop and build their organizations' Enterprise Architecture

1.5 Scope and Applicability of the NGEA

This framework provides a guiding reference for the deployment and implementation of Information Technology/e-Government systems in the FPIs. At the sub-national levels, State and Local Government bodies are encouraged to use the framework for their IT/e-Government systems deployment as parts of the federating unit to ensure Government Digital Transformation is achieved at all levels of government in Nigeria.

Therefore, the framework is applied to:

I. All Public Institutions (including Local, State and Federal Government);
II. ICT Product/Service Providers for public institutions;
III. Development Partners in partnership with Government; and
IV. General Public

1.6 Current State Analysis

The Nigerian IT/e-Government environment is in a Silo State where there is barrier in communication, information exchange and interoperability of IT systems between and across Public Institutions. The result of the survey conducted at the Strategic Capacity Building Programme for CEOs of Federal Public Institutions on August 09, 2018 revealed this. This scenario makes it difficult for Public Institutions to collaborate where cross-portfolio services are required. It is also making IT deployment and solutions costly in any attempt to initiate seamless communication, interoperability and integration of IT systems between government institutions.

The following shows part of the result of a survey conducted at the Strategic Capacity Building Programme for CEOs of FPIs on August 09, 2018.

The Survey: About One Hundred and Seventy-Five (175) participants attended the workshop and One Hundred and Six (106) participants responded to the survey questions. This represents 60.1% of participants. The survey was intended to measure Nigerian Government Enterprise Architecture Readiness and maturity as well as to make decision around most appropriate Operating Model (OM) for IT/e-Government deployment in the FPIs.

Analysis & Interpretation: The following presents part of the survey analysis & Interpretation:

1). The level of e-Government Maturity

Table 1.0: e-Government Maturity of FPIs

Maturity Level	Response (%)
Emerging Presence: Numerous Website offering basic information online	16.98

Enhanced Presence: More sophisticated sites with citizen interactions- email, social media and downloadable forms	66.04
Transactional Presence: Two-way interactive applications provide citizens with opportunities for online, financial and non-financial transaction	12.26
Connected Presence: The way government operates fundamentally change, and there is better coherence, integration and coordination of processes and systems within and across government agencies. Government transforms itself into a connected entity.	4.72

66.04 percent and 4.72 percent of FPIs are at the enhanced and connected stages of United Nations' e-Government maturity model respectively. The interpretation of this is that most of the FPIs have interactive websites that cannot offer complete transactions online for a service. Therefore, there is a need for a deliberate approach and action to move these categories of FPIs from enhanced stage to transactional and connected (transformation) stage. Not until this is achieved, the idea of WoG and Government Digital Transformation might be elusive. Furthermore, the earlier report on the Ministries websites' ease of doing business assessment conducted by the NITDA in June 2017 revealed that only 25 percent AND 37 percent of them has reachable phone numbers and email addresses respectively. This might be interpreted that 66.04 percent for enhanced presence stage might not be a true percentage but less than.

2). Description of Organization Strategy and Approach to ICT

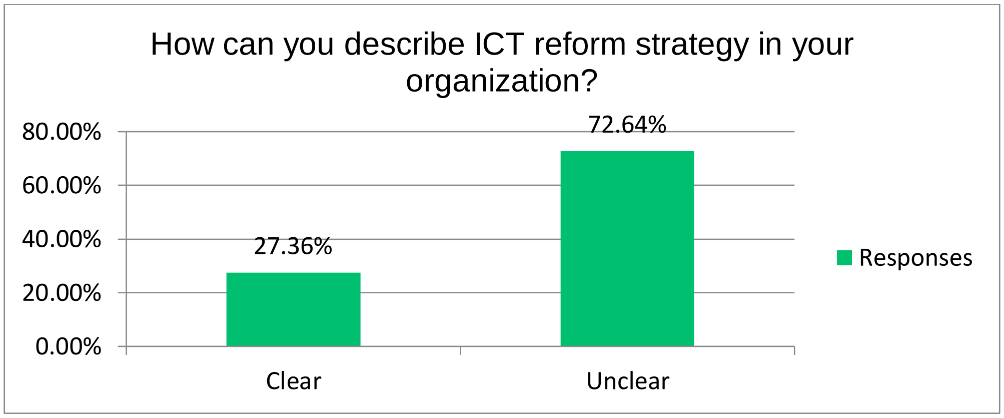


Figure 2.0: ICT reform Strategy

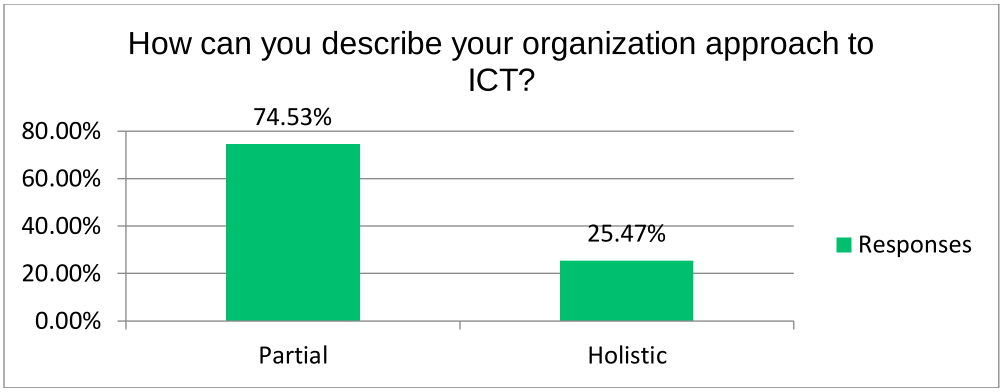


Figure 3.0: Organization Approach to ICT

72.64 percent of responded FPIs do not have a clear ICT reform strategy in their organization while 25.47 percent of responded FPIs have holistic approach to ICT in their organization approach to ICT. The implication of this is that ICT will have low pay off benefits and less optimal use of ICT applications and infrastructure deployment. This is the reason why there is a lot of wastage and high cost of IT investments with no correspondent value for money. For FPIs to derive maximum benefits from ICT their reform strategy must be clear and approach to ICT must be holistic.

4). The Choice of Operating Model

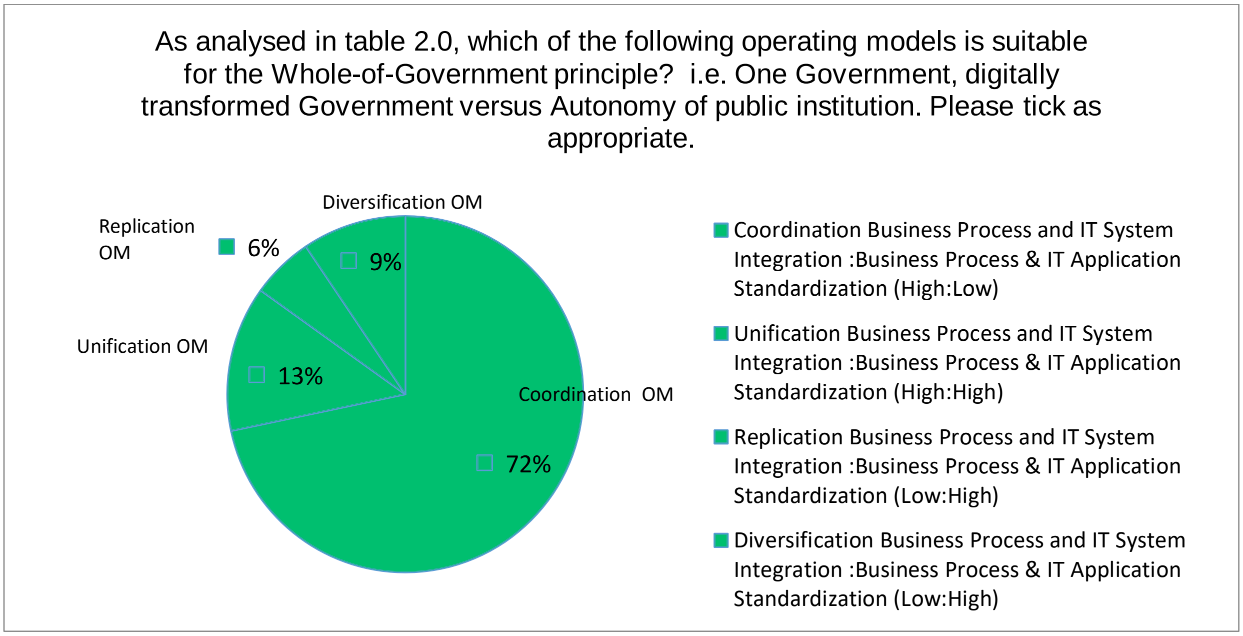


Figure 4.0: The Choice of a Suitable Operating Model for the Federal Government of Nigeria

Operating Model is the requirements with respect to the choice of the level of IT systems integration and standardization across the FPIs as a whole. It is a choice on how FPIs will deploy IT/e-government systems to achieve WoG and Government Digital Transformation agenda. Based on the explanation of the four Operating Models and their strategic choices, about 72 percent of FPIs chose coordination operation model. The interpretation is that FPIs have made a strategic choice of achieving a WoG without necessarily compromising their autonomies.

5). Agencies with Enterprise Architecture

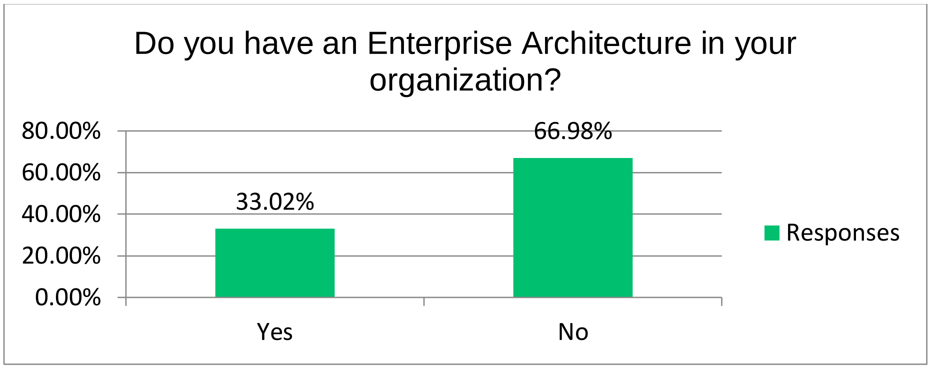


Figure 5.0: FPIs with Enterprise Architecture in place

66.98 percent of respondents indicated that they do not have Enterprise Architecture in place. This means most of FPIs do not have a guiding reference and road map for IT deployment and investment.

6. FPIs Readiness to Key into NGEA

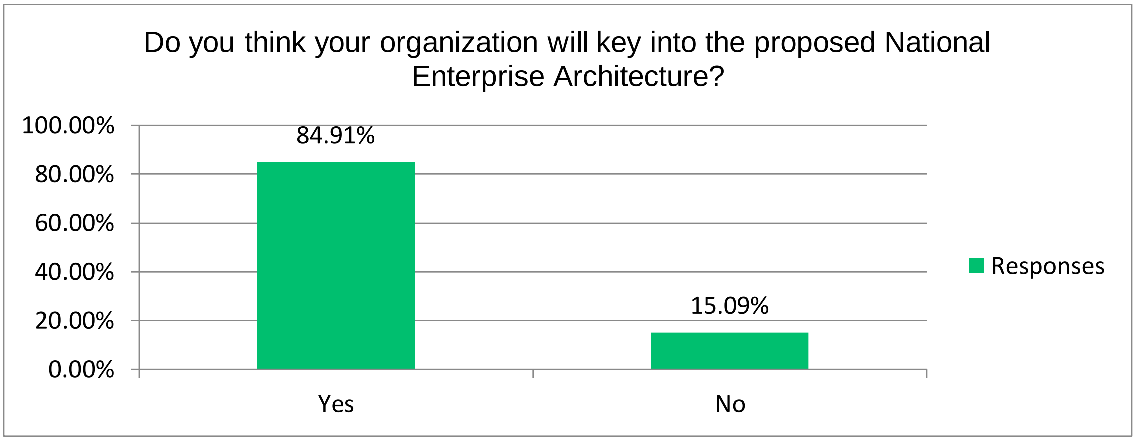


Figure 6.0: FPIs' support for National Enterprise Architecture

84.91% of respondents indicated interest to key into the National Enterprise Architecture programme. This means most of the FPI are not comfortable with the value they are currently deriving from IT investments and are ready to shift from the traditional ways of deploying IT in their organizations.

General Interpretation: The result indicated that state of EA and IT adoption and maturity in FPIs are varied. It is observed that majority of FPIs have generally low level of maturity with respect to architecture driven approach to e-governance. This inconsistency and inefficiency in IT deployment across FPIs is not healthy and sustainable for achieving Government's vision, policies, strategies, plans and programs. Moving from the current situation to a desired one requires adopting best enterprise practices, IT adaptation and contextualization to Nigerian environment. Therefore, the decision of Coordination Operating Model will greatly help the country's enterprise architecture in achieving WoG and GDT as well as the respect for the autonomy of FPIs to make independent IT applications and services decisions based on their functions and mandates.

1.7 Authority of the NGEA

In exercise of the powers conferred on NITDA, specifically by section 6 (a) and (c) of the National Information Technology Development Agency Act of 2007, the Nigerian Government Enterprise Architecture Framework (NGEAF) is hereby issued. The NGEA serves as a guiding reference for IT system deployment in the public institutions. This Framework is an abstract from which concrete implementation of Enterprise Architecture can be derived government-wide or used by individual Public Institution to develop enterprise architecture.

SECTION TWO: The Path to Government Digital Transformation (GDT) in Nigeria

2.1 The Future State

The long-term target of NGEA for the country is a One Government Enterprise (Whole-of-Government) that paves way for Government Digital Transformation agenda. This target requires deliberate and concerted efforts of every Public Institutions to follow every specification and requirement of NGEA.

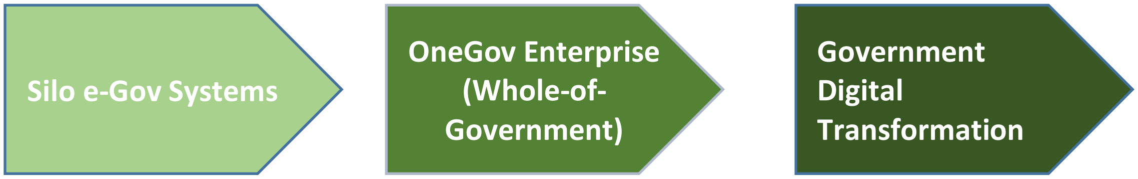

Silo e-Gov Systems
OneGov Enterprise (Whole-of-Government)
Government Digital Transformation

Figure 7.0: Transition stage for e-Government

2.1 The NGEA Vision

The vision for NGEA is to become the number one reference framework for the evolution and transformation of Nigerian Government IT system and environment from silo-based to a more efficient, integrated and sustainable enterprise. The process of transformation is a path of silo to One Government (Whole-of-Government) Enterprise and eventually to Government Digital Transformation.

2.2 NGEA Value Proposition

The strategic value proposition that makes NGEA different from other Government Enterprise Architectures across the world is its ability to incorporate two quite distinct expectations:

1. **1Gov, Whole-of-Government Agenda**: This is the ability of public institutions' ICT systems and other resources to work cooperatively to deliver cross portfolio services for customers in an integrated manner. This brings convenience, reduces cost of service delivery and taking, encourages quick response to citizens' queries and participatory governance, transparency, and sustainability among others.
2. **The autonomy of each Public Institution**: Respect for the autonomy of FPIs' in making certain critical decisions as they affect their mandates and functions is critical to sustainability of NGEA, building cooperation and trust among FPIs; and in return promotes sustainability of ICT projects in the public sector.

There are a lot of requirements to achieve the value proposition; they are discussed in the next chapters. However, there is a need to define a maturity model and different stages to give a clear roadmap to achieve the value proposition and attain the vision.

2.3 NGEA Maturity Model and Stages

EA maturity is a gradual shift in how resources are channeled into IT investments and business process redesign. EA Maturity defines the current levels of different public institutions' architecture at supporting a whole-of-government and digital transformation initiatives. It can be used to assess the current government-wide enterprise architecture to know the extent to which it can support a whole-of-government and digital transformation vision.

The findings from the analysis of the survey in section 1 reveal that effective communication and information exchange, interoperability of IT systems between and across FPIs still pose serious challenge. It also indicates that FPIs' e-Government maturity are at different stages with higher percentage of the Institutions at the 2nd stage (Enhanced) of the United Nations e-Government Maturity model.

This situation buttress the fact that the manner and ways many public institutions have built their processes and IT systems over time are not appropriate for the WoG and GDT new vision. Government digital transformation requires reengineering of core processes and systems even as public institutions depend on the processes and systems to complete their daily operations. WoG calls for the need to **redesign** and **implement new systems**, **processes,** and **IT infrastructure** without sabotaging daily operations. However, Government cannot shut down its businesses and start from the scratch during the transformational stage.

Adapting the Research by MIT CISR indicates that there are **predictable patterns** and path for government to follow as it navigates the trans

formation processes in achieving a WoG and Government Digital Transformation. The consistent pattern for advancing EA is labeled in four stages of EA maturity model. It proved that FPIs go through four different stages of information technology development to accomplish WoG. Figur 8.0 highlights the different EA maturity stages. At a minimum, WoG requires attainment of Optimized Core stage but the ultimate goal of any public institution and the WoG is to attain service modularity stage leading to Government Digital Transformation.

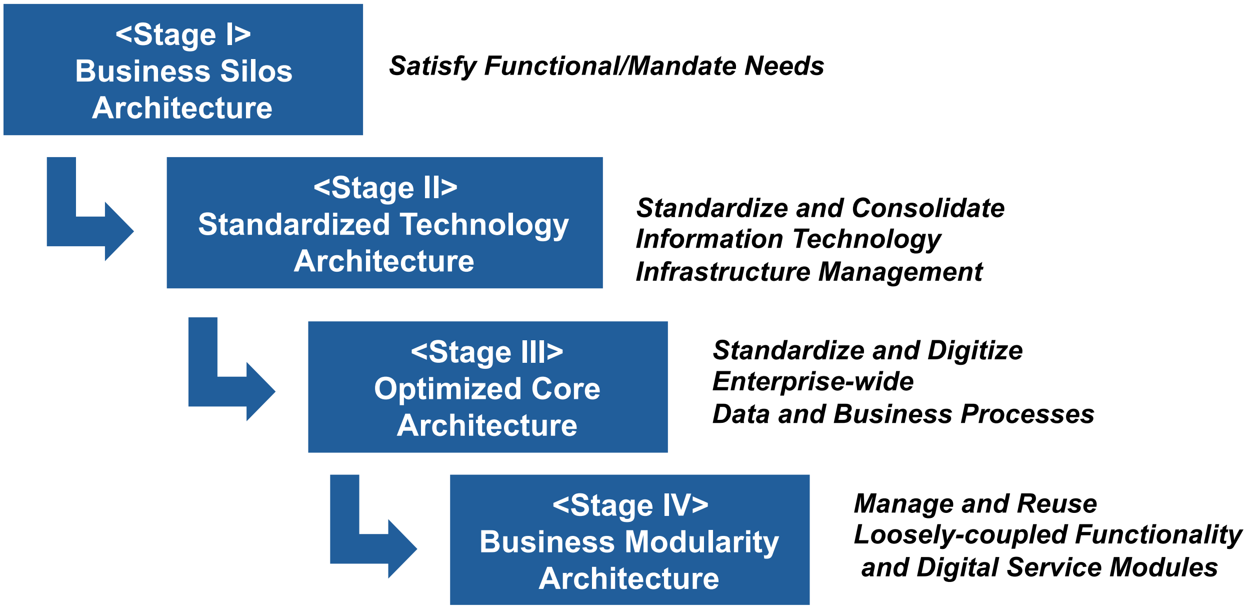


Figure 8.0: Enterprise Architecture Maturity Stages.

The different evolutionary stages are explained as follows:

NOTE: The explanations here follows that of research by MIT CISR in Enterprise Architecture As a Strategy

2.3.1 Business Silos Architecture Stage: At Silo stage, each public institution is focused on maximizing its IT systems to deliver its independent strategic initiatives and functional needs. It is stage where individual builds its IT infrastructure according to its needs, **independent of a common standard**. The role of IT is to **automate organization-specific business processes** and **functions** that meet its requirements. The key driver of the Silo stage is achievement of specific business functions/mandates.

These one-off solutions, however, create a legacy of systems that are difficult to integrate with each other or at best integration occurs within the organization IT systems without provision for government-wide interoperability requirements. Integrating across the government is complex, costly and requires resources and deliberate efforts to collaborate. This desire for integration and a whole-of-government vision force every government to move to the standardized technology stage.

The aim of IT investment at the Silo stage is operational efficiency of each public institution and increase in revenue generation.

2.3.2 Standardized Technology Architecture Stage: The desire for integration and government-wide interoperability necessitates an efficient IT environment across public institutions and their partners. **IT efficiency** is provided through **technology standardization** across the government and eventually leads to **centralized technology management** in most cases. Public institutions begin to shift some of their IT investments from **local applications** to

shared infrastructure. The aim is to establish **technology standards** in order to decrease the **number of platforms** each public institution manages. **Fewer platforms mean lower cost.**

The role of IT in the standardized technology stage is to **automate each public institution's business processes** with a major shift toward centralized **IT infrastructure management** in order to leverage on the **economy of scale** of IT infrastructure's capabilities. The focus is on **cost-effectiveness** and **reliability of government's IT systems**. At this stage, IT projects and business solutions must be in accordance with the established technology standards. The needed efficiency is gained through the introduction of **standardized and consolidated technology platforms** and provision of **shared infrastructure services**. Business solutions and applications leverage IT infrastructure and technology platforms to deliver innovative solutions.

The design of any IT projects and solutions must align with the acceptable technology standard and platforms. **Instead of defining solutions to deliver public services and looking for technology that best delivers that solution, government in this stage negotiate the best possible solution** given the **acceptable technology** platforms. The commitment to technical standards means that the IT application representing **the best fit in terms of functionality** may be rejected because it doesn't work with the whole-of government's **technology architecture and standardization** requirements.

The fact that technology standardization **reduces risk of IT Infrastructure implementation** by different organizations and cost of **shared services** (in the areas of support, maintenance, and purchasing) as well as improves **reliability, security and development time** does not readily overcome the business **silos problem of data embedded in the legacy applications**. Even though technology standardization increases access to shared data by introducing **data warehouses**, **transaction data is still embedded in individual legacy applications**. This stage prepares governments for optimized core stage.

NOTE: Standardization is a collaborative effort and is driven by government policy and IT regulation. The compliance to standardization is also a collaborative effort which is driven through IT engagement model.

2.3.3 Optimized Core Architecture Stage: In Optimized Core Architecture stage, the drive is toward appropriate government-wide data standardization and process integration. Organization move from local or **each organization's view of data** and application to government-wide view. There are standard approach(es) for extracting **needed transaction data** from individual applications in different public institutions and make the data available for the **provision of cross-portfolio services.** Thus, IT investments consideration is shifting from organization-specific local applications and shared infrastructure to **shared data and WoG systems**. This stage is where coordination operating model becomes feasible and operationalized. Data becomes more transparent and common processes and functionalities become more comparable and predictable.

The focus of government is to digitize all its core data and business processes in an optimized manner. Once this is achieved, changes to government's data becomes more difficult but building applications to create new digital services on government's IT infrastructure becomes easier and faster. The role of IT in the optimized core is to facilitate achievement of government-wide objectives of building a WoG for **digital services.** The WoG strategic advantage is built on this foundation.

One good thing about standardized shared data promoted by coordination model is that it does not take control of business process design peculiar to each public institution, instead the optimized core promotes innovation, creativity in digital services that are citizen-centric and citizen-driven either as individual organization or as a WoG. One major characteristics of the optimized core is the availability of National Identity Database System. Optimized core paves way for data and core business process reuse.

2.3.4 Service Modularity Architecture Stage: In Service Modularity Architecture stage, public institutions manage and reuse loosely coupled digital service components to preserve enterprise-wide standards while enabling local (each public institution specific) differences. It ensures that governments continue to refine and increasingly **modularize the processes and shared data that were digitized in the optimized core**. This represents the ultimate goal of the coordination architecture and NGEA. The service modularity architecture enables **strategic agility** through **customized or reusable functionality and service modules.** This is achieved through technological concepts such as **"web services"** built via standardized interfaces to access the shared data and services across government and/or direct integration of applications with shared/back-end data.

The role of **IT in service modularity architecture is to provide seamless linkages between reusable modules (applications) and the shared data**.

The benefits of the optimized core stage, that is **efficiency** (responsiveness, agility etc.) and **single face to customer** (i.e. one-stop shop, single-window, **pr**ocess and data integration), is extended by modular architecture. **Modular architectures provide a platform for innovation**. In addition, **modular architecture enables local experiments**, and the best one can be spread throughout the WoG. Quickly developed and very focused add-on modules allow strategic experiments that respond to changing citizen's requirements and needs. At this stage, public institutions reuse expertise in process, data, and technology standardization gained in the earlier stages.

2.4 Navigating the Enterprise architecture Maturity Stages

Research has found that to achieve WoG and GDT, stages cannot be skipped because of the **major IT and organizational change** involves in each stage. WoG architectural change is a function of collective changes experienced by each public institution in the architectural processes. The major requirements for the WoG architectural change is that all the FPIs must agree on the change and then they need to simultaneously implement the change at their pace. Therefore, government policies and IT regulations drive this change.

As government migrates from each architectural stage; the ultimate goal is to **change focus from specific** organization to **government-wide optimization.** Migration from business silos to standardized technology allows for government-wide flexibility by reducing technical complexities and thus reduces implementation time. Attaining Optimized core means that each public institution loses maximum control and responsibility over shared data and sometimes IT systems that execute them. When service modularity stage is reached, flexibility grows both locally (within each public institution) and government-wide (WoG). With a solid platform for technology standardization and shared data, public institutions can plug-and-play functionality modules which makes changes simpler to implement.

Table 2.0: EA Maturity Description

	Business Silo	**Standardized Technology**	**Optimized Core**	**Service Modularity**
IT Capability	IT serves organization-specific functions/ Mandates	Government-wide technology standards	Government-wide Digitized & standardized Data and business process	Plug and Play functionality modules and digital services
Business Case for IT	Organization specific ROI from IT and operational effie	Reduced organization and Government-wide IT costs; improved WoG interoperability requirements	Improved organization and government-wide business performance; improved WoG integration requirements	Government Responsiveness and Strategic agility
Key Management Innovation	IT-enabled change management	Standardization and Exception monitoring, compliance and management	WoG strategic support for shared data and digital services	Organization and Government-wide Strategic support for reusable functionality modules and digital services
Locus of Control	Local control of business functions/ mandates and business processes.	Shift toward centralized IT infrastructure management and shared services	Data and services are shared	Controls are shared among public institutions and WoG requirements
Key IT Governance Issues	Measuring and communicating IT value within each organization	Establish organization and government-wide IT infrastructure responsibilities	Align organization and government-wide shared data and services responsibilities	Leadership innovation
Strategic Implications	Local/functional optimization	IT efficiency	Organization and WoG operational efficiency	Organization and WoG service responsiveness

2.5 The Principles of the NGEA

The following guiding principles form the foundation and basis upon which NGEA is built to also navigate the stages and build the right enterprise for Government Digital Transformation (GDT):

1. **Partnership & Collaboration**: This principle focuses on harnessing opportunities inherent in comparative advantage and strength of each partner when IT projects are implemented to ensure high success rate. FPIs are enjoined to seek for every viable opportunity to partner and share resources in support of a common goal and vision of WoG and GDT.
2. **Interoperability & data exchange**: Data is critical to public service delivery. Having a single view of citizens' data and ability to share and exchange data seamlessly across government determines the maturity of a country's e-Government system. Interoperability of e-government systems at organizational, semantic and technical levels enhances data exchange as well as promotes convenience and innovations in service delivery.
3. **Simplicity:** One of the strategic targets of NGEA is simplification of enterprise architecture documentation, development processes and implementation. Experience has shown that most enterprise architecture projects ended up in the shelves. NGEA tends to deviate from the complexity and proposes public institutions' friendly architecture that is easier to implement.
4. **Efficiency**: Efficiency is at the heart of the NGEA. It aims to promote efficient IT environment that promotes high quality, low cost and on time delivery of IT projects.
5. **Capability:** Another strategic target of the NGEA is to promote the needed capacity required to deliver value from every IT project in the public sector. Capability is a complete set of capacities, skills imbedded in people, process, and/or technology and efficient use of these resources by FPIs to execute their mandates and mission.
6. **Local Content & Context**: Another strategic aim is the promotion of local content in ICT through NGEA. Indigenous ICT players are critical to the development of Nigeria ICT industry. NGEA is developed to give strong support for local ICT industry and ensure that indigenous ICT players have better chance in implementing ICT projects in Nigeria.
7. **Alignment**: The NGEA is used to promote alignment between IT and FPIs' mandates/businesses (including public service culture & structure, processes, technology and people). Such alignment ensures expectation from ICT projects are met and every FPI implements ICT projects that are aligned to their functions.
8. **Sustainability**: The NGEA will ensure that every ICT projects is sustainable in terms of cost, terms and conditions for licenses, quality, capacity and capability and in strong support for local content.

2.6 The Structure of the NGEA

Every Public Institution in Nigeria has statutory mandates/functions as an integral part of the overall Government's responsibilities to the country. Those mandates/functions are translated into specific services that must be delivered to the Government's customers (citizens, businesses and public institutions). Public Institutions are to build appropriate **digital capabilities** required to deliver those services efficiently on individual basis and as a Whole-of-Government. Building these capabilities necessitates Public Institutions to **hire appropriate people; adopt and use appropriate technologies** as well as **define, streamline and digitize specific processes considering global best practices and the country's political, institutional, regulatory etc. contexts**. These capabilities should also enable public institutions to provide cross portfolio services seamlessly with the aid of IT infrastructure and applications already deployed or that will be deployed in the future.

On that note, there are two key information technology trendy terms to be observed when building digital capabilities: **standardization** and **integratio**n. The digital capabilities comprise of **business process, IT systems (infrastructure, government data & core applications) and e-Government services/e-Services applications standardization and/or integration**. Standardizing common business processes, IT system (infrastructure) and **e-Government services/e-Services applications** ensures achievement of the following objectives: **reusability, interoperability, reduction in the cost of IT systems, and efficiency in IT implementation**. Data and IT systems integration ensures achievement of the following objectives: **breaking of silo systems and enabling of common view of an enterprise data and information**. These are one of the main objectives of NGEA.

For the public institutions to develop these capabilities on individual basis and/or as a Whole-of-Government for efficient delivery of services, the current IT/ICT environment must be reorganized, strategic choices must be made and **subsequent deployment of IT/ICT must follow best practices**. This entails thinking globally by adopting empirically proven and practicable best practices and act locally by considering Nigerian situational contexts and environment. It has been proven by the Center for Information System Research (CISR), through an extensive research conducted across private and public organizations, how big and successful enterprises developed and built digital capabilities necessary for enterprise change and transformation. The result of the research showed how strategic choices and best practices in IT adoption and application have been a critical success factor for business and governance transformation. The result was able to prove how IT as a strategic asset is shaping immediate and future opportunities for successful businesses and governments.

The strategic choices and best practices with consideration for environment and situational contexts are embedded in three things which an enterprise must learn to build foundation for execution and digital capabilities essential for government digital transformation.

The three strategic components are:

1. Operating Model;
2. Enterprise Architecture Framework; and
3. IT Engagement Model

The Nigerian Government Enterprise Architecture is built on this structure. The prescriptions, strategic choices made and best practices adopted at each architectural layer considering the country's context and environment are explained in the next section. Furthermore, the NGEA value proposition of OneGov (Whole-of-Government) and respect for each FPI mandates/functions is a critical reference and prescriptive guide at each layer of the structure. The structure is depicted in figure 9.0.

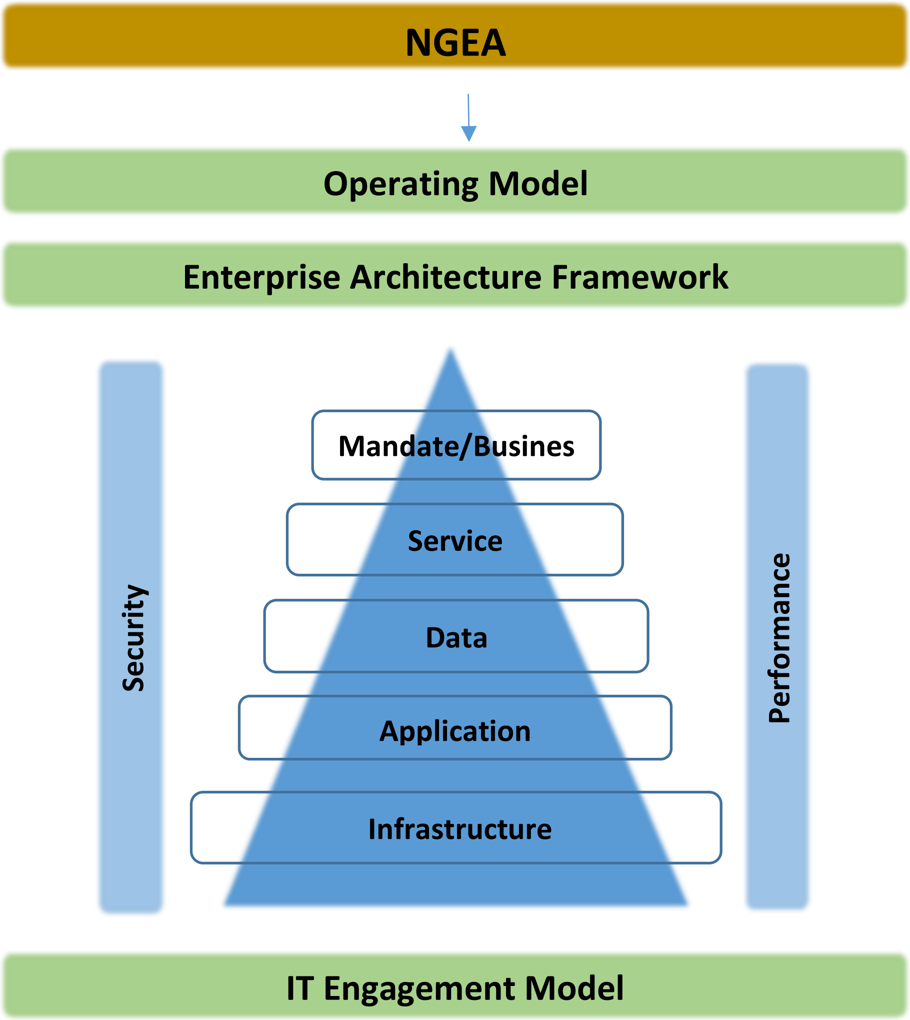


Figure 9.0:: Nigerian Government Enterprise Architecture Framework

SECTION THREE: The Core of the Nigerian Government Enterprise Architecture (NGEA)

As explained in the previous section, the core of Nigerian Enterprise Architecture are **operating model, enterprise architecture framework** and **IT engagement model**. The strategic choices made, best practices adopted and prescriptions at each layer of the NGEA structure are enunciated as follows.

3.1 Nigerian Government Operating Model

Operating Model is the necessary level of data, business process, IT systems and e-Government services/e-Services applications integration and standardization necessary for efficient public service delivery to customers (Citizens, Businesses and Government) either as single public institution or Whole-of-Government. **Integration** is the agreement on the extent to which the Whole-of-Government will share data and IT systems (extent of government-wide interoperability) while **standardization** is the agreement on the extent of standardizing e-Government service/e-Service applications (independent IT/e-Government applications decisions by public institutions) and business process (autonomy of FPIs to define business processes that suit the kind of services they provide in line with their statutory mandates/functions).

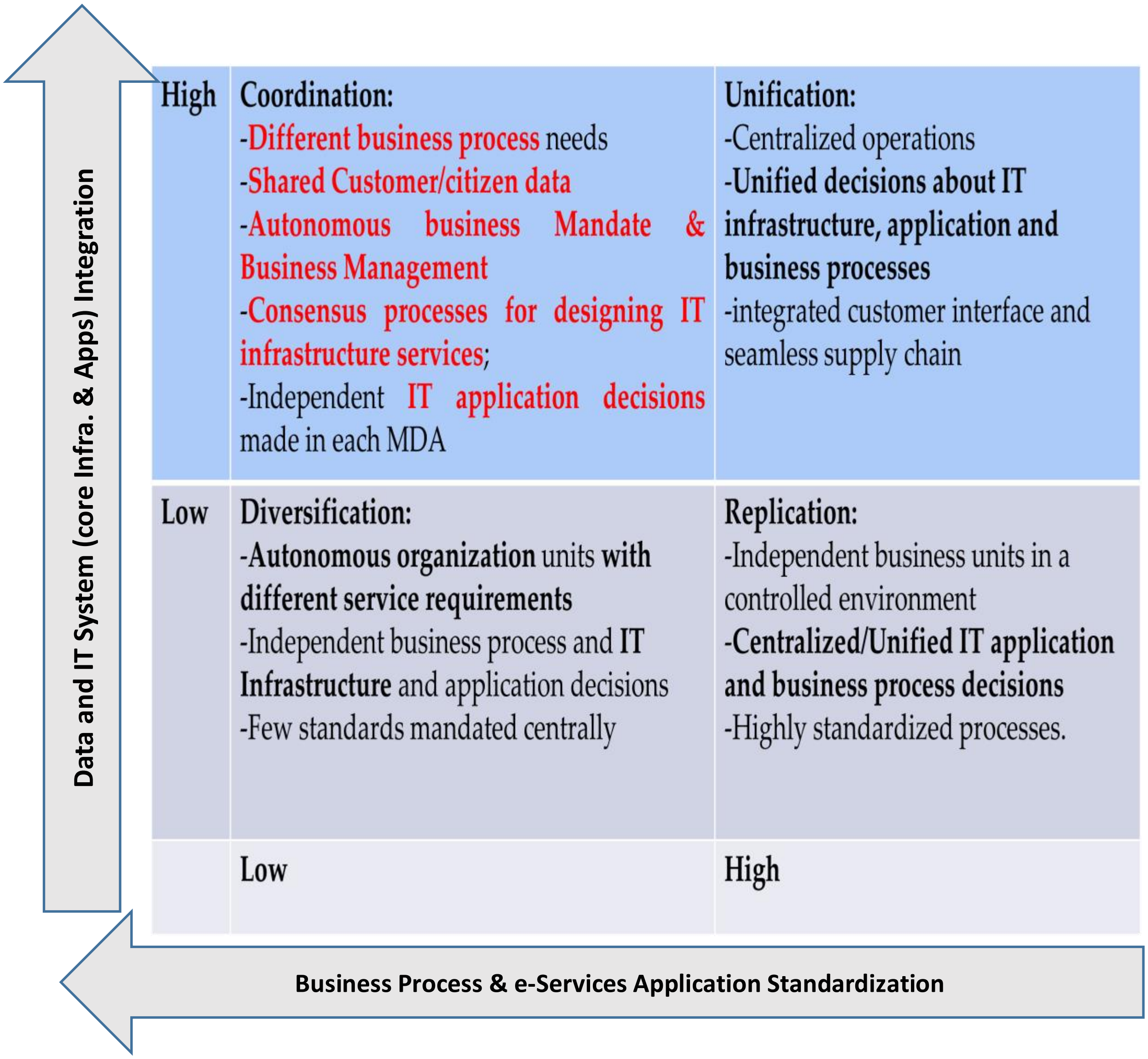
The figure 9.0 describes four possible operating models in which a strategic choice of one would be made based on its suitability for the country. The strategic choice on the suitable operating model for the country, considering the value proposition (upon which the NGEA is founded, that is Whole-of-Government and sacrosanct of FPI autonomy in making certain independent decisions) was made by the FPIs' CEOs at the e-Government Strategic Capacity Building in August 09, 2018. The analysis of the administered questionnaires is presented in NGEA vision. The table 2.0 also indicates pattern of responses to the question on the choice of the operating model.

Table 3.0: Operating Model Description with response

Operating Model	**Data and IT System (Data, Infra. & Apps) Integration** [Required level of interoperability among FPIs] **:** **Business Process &e-Service Applications Standardization** [Required level of common business process and e-Services application standardization]	**Response (%)**
Coordination	High : Low	71.70
Unification	High : High	13.21
Replication	Low : High	5.66

Diversification	Low : Low	9.43

The coordination operating model received the highest score among the four operating models which indicated FPIs' readiness for Whole-of-Government-**One Government** (exchange data and share IT systems) however, they want to be solely responsible for decisions on digitizing their business processes and services in alignment with their mandates and functions.



Data and IT System (core Infra. & Apps) Integration

High

Coordination:
-Different business process needs
-Shared Customer/citizen data
-Autonomous business Mandate & Business Management
-Consensus processes for designing IT infrastructure services;
-Independent IT application decisions made in each MDA

Unification:
-Centralized operations
-**Unified decisions about IT infrastructure, application and business processes**
-integrated customer interface and seamless supply chain

Low

Diversification:
-**Autonomous organization** units **with different service requirements**
-Independent business process and **IT Infrastructure** and application decisions
-Few standards mandated centrally

Replication:
-Independent business units in a controlled environment
-**Centralized/Unified IT application and business process decisions**
-Highly standardized processes.

Low

High

Business Process & e-Services Application Standardization

Figure 10.0: Description of Operating Models

The implication of this is that, there is a need for high level of data and IT systems interoperability (i.e. high interoperability requirements for Core IT infrastructure and applications) integration to achieve a Whole-of-

Government while low level of business process and front-end applications standardization is required across FPIs to guarantee their autonomy. High integration implies high level of interoperability requirement and low standardization means high level of control by FPI on the choice of their operations. This is represented in figure 10.

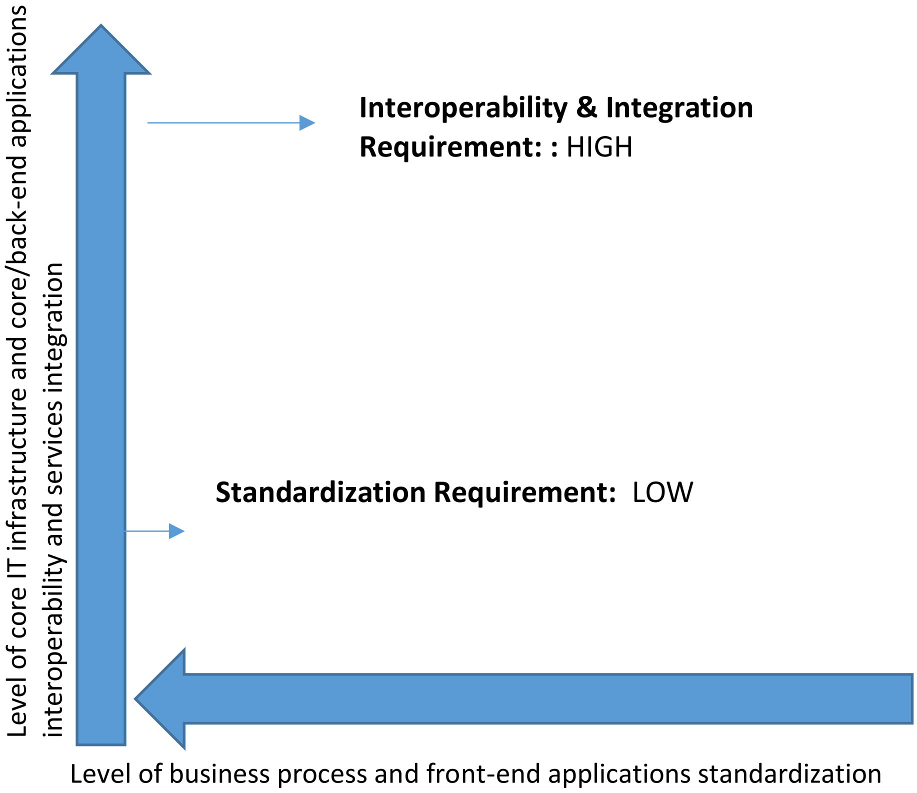

Level of core IT infrastructure and core/back-end applications interoperability and services integration
Interoperability & Integration Requirement: : HIGH
Standardization Requirement: LOW
Level of business process and front-end applications standardization

Figure 11.0: Level of IT Systems, BP and Service interoperability and standardization

3.2 Description of Coordination Model

The Coordination Model supports the position of the FPIs as indicated in the result of the study and the value proposition for NGEA. This model allows FPIs to make their business process and front-end IT applications' decisions independently based on their mandates and strategic directions with less standardization while consensus is required at making decisions on core IT infrastructure and core/back-end applications to ensure attainment of the required level of service integration and data sharing for the Whole-of-Government. Data exchange and sharing is the most important requirement for interoperability and service integration. The core diagram for Coordination Operating Model is depicted in figure 11.0.

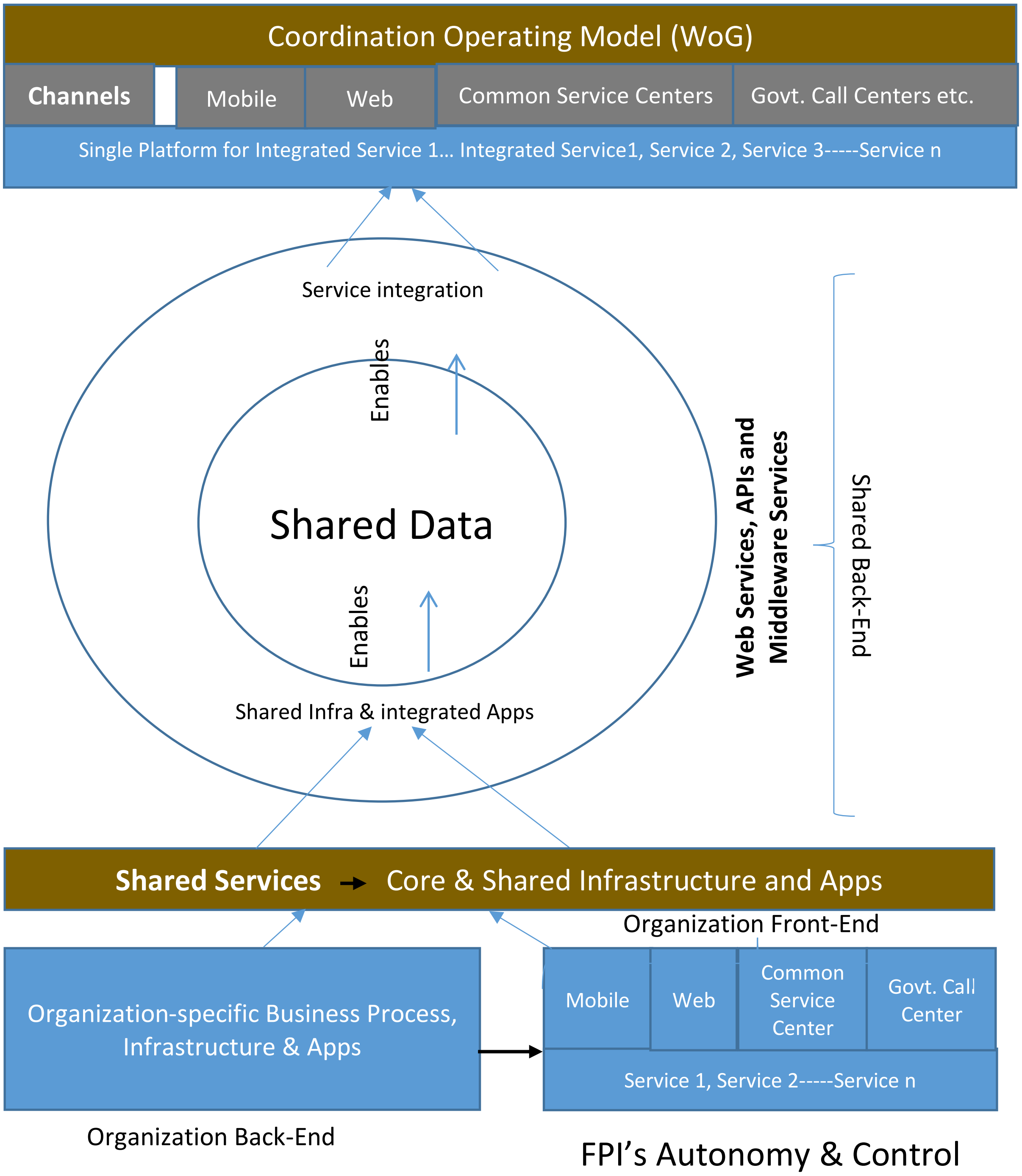

Coordination Operating Model (WoG)
Channels
Mobile
Web
Common Service Centers
Govt. Call Centers etc.
Single Platform for Integrated Service 1… Integrated Service1, Service 2, Service 3-----Service n
Service integration
Enables
Shared Data
Enables
Shared Infra & integrated Apps
Web Services, APIs and Middleware Services
Shared Back-End
Shared Services
Core & Shared Infrastructure and Apps
Organization Front-End
Organization-specific Business Process, Infrastructure & Apps
Mobile
Web
Common Service Center
Govt. Call Center
Service 1, Service 2-----Service n
Organization Back-End
FPI's Autonomy & Control

Figure 12.0: Core Diagram for Coordination operating model

The coordination operating model guides what and how specifications are defined in each layer of the enterprise architecture reference models in section three (3) based on the NGEA vision, principles and value propositions.

The core diagram and coordination operating model guides the Federal Government on how IT should be deployed and adopted, how to enhance each layer of the enterprise architecture framework and grow enterprise architecture maturity as each IT project is being added one at a time by each Public Institution. It requires a whole lot of shared data and back-end services within and across public institutions and at same time allow indiviupublic institutions at the federal level to make decisions on their own business processes and front-end applications.

Thus, each IT projects by FPI (if the specifications of NGEA is followed) will help build a sustainable National Enterprise Architecture that addresses the current challenges of IT deployment in the public sector. The IT engagement model ensures NGEA principles are followed and upheld as each IT project is implemented one at a time.

The eventual result of these processes is an Enterprise (Nigeria) where desired outcome of IT adoption is significantly manifested in the efficiency, productivity, governance, growth and competitiveness for socio-economic development of the country. This stage is tagged Government Digital Transformation (GDT).

3.3 Enterprise Architecture Reference Models

The reference models form an abstract framework for explaining, prescribing and understanding significant relationships among enterprise entities (majorly IT and other entities such as business process, people, organizations' capabilities etc.) and how these entities are fixed and aligned together to enable desired outcome. It provides consistent models, standards or specifications supporting IT enablement capabilities and opportunities for sustainable WoG and GDT.

The model is independent of specific standards and technologies rather support open implementations that promote interoperability, scalability and innovations. It comprises of the specific layers in figure 13.0. Therefore, the model explains what is expected of Public Institutions at each distinct layer while implementing IT projects to ensure consistency and take care of flexibilities that could arise as a matter of necessity. Each layer relates to another layer and are interwoven to enable the needed capabilities and opportunities.

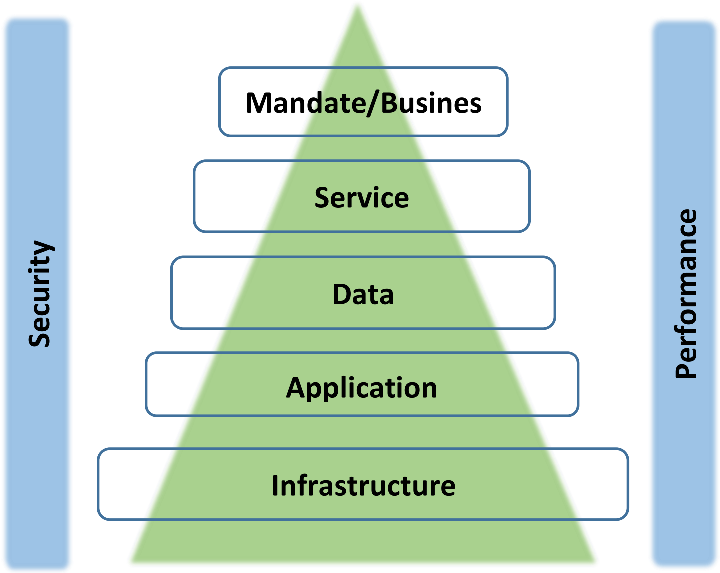


Figure 13.0: Enterprise Architecture Reference Model

The prescription of the reference model is as follows:

3.2.1 Business Architecture Reference (BRM) Model

Introduction and Purpose*:* Business reference model provides framework for business-oriented prescriptions of each public institution's mandates/functions in relation to IT, that is, proper alignment of public institution's business (mandates/functions) with IT. Strategic alignment of business and IT enables each public institution's to deliver expected value to its customers. The BRM promotes independence of each Public institution and cross-government collaboration. It enables public institutions discover opportunities for cost savings and new business capabilities that help them achieve their strategic objectives.

The purpose of BRM is to

a. Provide standardized way of classifying government business in terms of functions/mandates. It also provides public institutions with a standard means to categorize their capital investments, identify areas for collaboration, consolidation and reuse based on the business functionality being delivered, and help improve the overall IT architecture to better enable mission outcomes;

b. Provide framework to describe and analyse public institutions' business areas and IT applications that are suitable for their business operations; and

c. Help public institutions reduce wastage, improve performance, increase return on every investment and ensure value for money on every public expenditure.

NGEA High-Level Expectation of Business Reference Model: The following highlights at high-level what is expected of BRM. This expectations are what each public institution and national IT governing structure must work to achieve as each IT project is being added to the enterprise (Nigeria). The BRM sets strategic direction for adoption of IT in governance and business operations of government.

a. ***Uphold ONE Government and Autonomy of Public Institutions***: BRM is to complement WoG Operating Model i.e. Coordination Operating Model which supports ONE Government idea and at the same time encourages public institutions autonomy. Public institutions are expected to use BRM to promote policies and strategic directions that allow IT to support this value proposition.

b. ***Mandates/Functions and IT Projects Alignment***: BRM is a framework for aligning public institutions vision, goals, policies, programs, plans, strategies and IT projects to guarantee expected public value with much positive impacts on the well-being of the citizens through opportunities maximization.

c. ***Promoting Enabling Business Environment***: One of the greatest challenges hindering the growth and diversification of Nigeria economy is poor enabling business environment. ICT is a major enabler of business environment. Therefore, public institutions are expected to use the BRM to promote policies, strategies, programs and projects that support enabling business environment.

d. ***IT as a Strategic Asset for Government Organizations and Businesses***: BRM is to re-orient government's perspective of IT of being an ordinary enabling tool to a strategic asset for shaping existing and future strategic opportunities of public institutions and the WoG.

The BRM Abstract Model

The Federal Enterprise Architecture Framework (FEAF) structured business reference model into three-tiered hierarchy representing **business areas**, **line of business** and **sub-functions**. The **business area** is the highest-level and it is composed of **lines of business**. Each line of business is further divided into business capabilities comprising of collection of specific business functions.

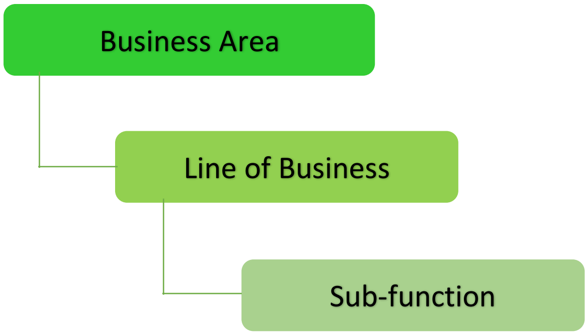


Figure 14.0:: The BRM Abstract Model

Table 4.0:Explanation of BRM Abstract Reference Model

Level	**BRM**	**Description**	**Example**
Level 1	Business Areas	Form the different social, political and economic sectors/industries or entities in the country.	**Sector:** Economy, Transport, Health, Security etc.
Level 2	Lines of Business (LoB) (within each Business Area)	Relate to specific functions/mandates in a business area. Lines of business are more of established public institutions with statutory functions/mandate	**Economy:** e.g. Public institutions responsible for Tax, finance etc; **Transport**: e.g. Public institutions responsible for Road, rail or air (aviation) transport; **Health**: e.g. Public institutions responsible for medical, pharmacy etc.; **Security**: e.g. Public institutions responsible for Policing, military, civil defense etc.

Level 3	Business Sub Functions (under each LoB)	Relate to sub-functions that enable lines of business carry out assigned mandates.
		
		Business sub-functions are more of departments/units or special purpose mechanisms to carry out specific tasks for line of business
			Economy: Accounting, finance etc. functions/departments/units;
			
			Transport: highways, passenger-handling, maintenance service, Reservation and ticketing functions/departments/units;
			
			Health: Cardiology, Surgery etc. functions/departments/units;
			
			Security: Intelligence & Investigation, training & logistics etc. functions/departments/units;

At the organizational level (each public institution), the business capabilities are represented by statutory services in which the organization was established to deliver. A set of business processes is, in turn, required to deliver those services. The **business operation** and **structure** are linked to the business processes supported by **service components** that are described in the Service Reference Model.

Major Driver of Business Architecture: Each business area (specific sector or industry) should be driven by **national plan/agenda** of the government and **WoG Operating Model (WOM)** for e-Government. A major concern here is to ensure there is always alignment of national plan/agenda, WOM and Information Technology.

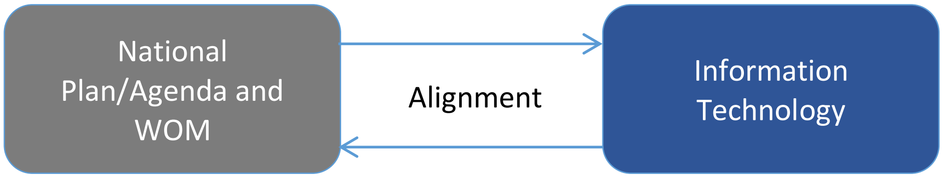


Figure 15.0: Business and IT alignment

Building Blocks for Line of Business: The following presents major building blocks of the business reference model for every line of business:

Enterprise's aspirations: (its **Vision**) –refined into **Goals** and **Objectives** –(called the Ends)
Enterprise's action plans: for how to realize them (its **Mission**) –refined into **Strategies** for approaching Goals, and **Tactics** for achieving Objectives (called the **Means)**

An enterprise, however, cannot operate on this Model of ends and means alone. The business needs to take into account the numerous **Influencers** that can hinder or assist its operation.

Influencers can provide **Opportunities** that would help the enterprise operate, as well as **Threats** that would thwart it. Influencers also represent **Strengths** the enterprise could exploit, or **Weaknesses** that it should compensate for. Whether Influencers are Strength, Weaknesses, Opportunities or Threats is determined by **Assessments**.

Once an Assessment has identified relevant Influencers in terms of their **impact** on Ends and Means, **Directives** (**Business Policies and Business Rules**) can be put in place to govern and guide the enterprise **Courses of Action** for delivering functions/mandates. All these influences sun-functions and determines how public services are delivered efficiently or otherwise.

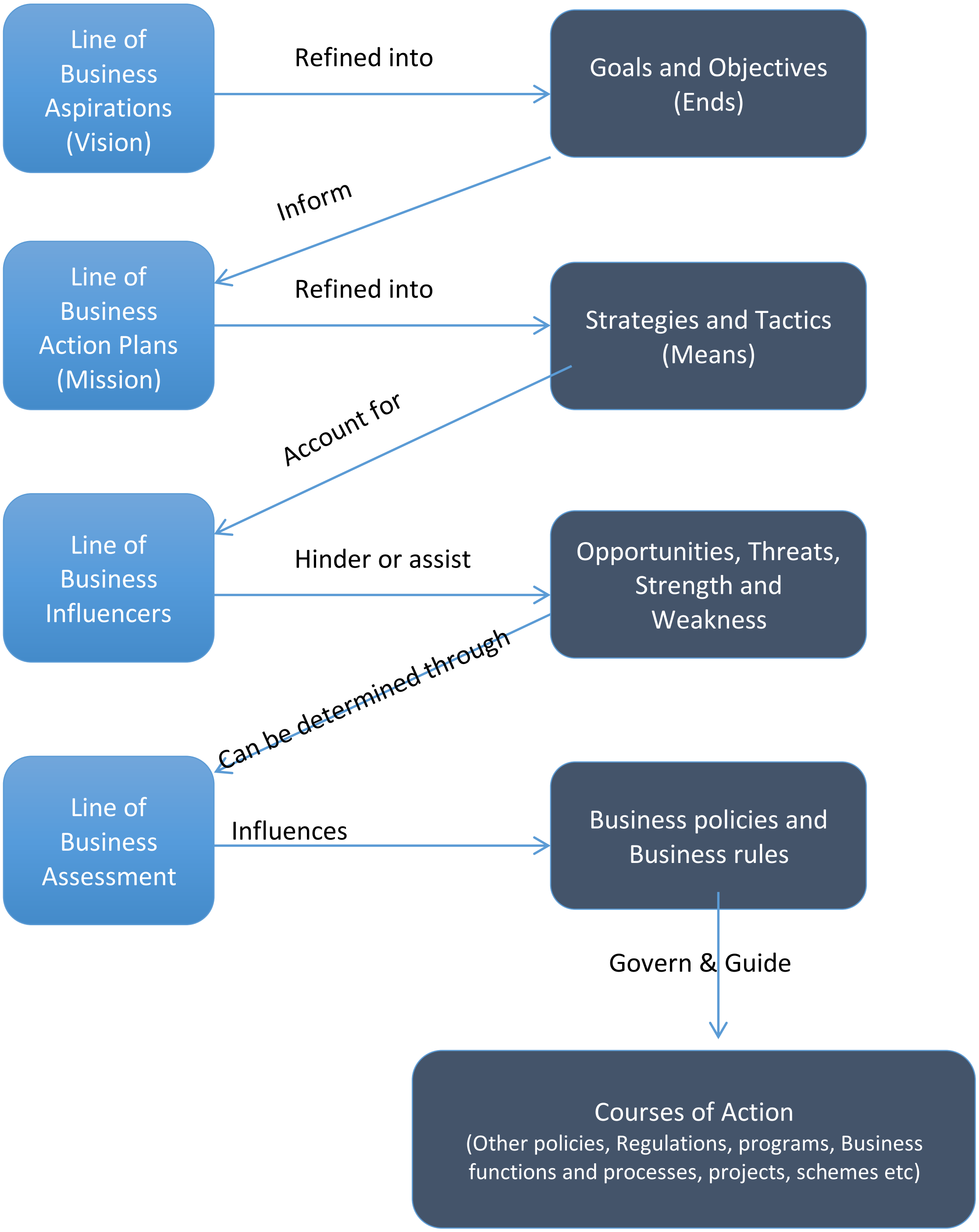

Line of Business Aspirations (Vision)
Refined into
Goals and Objectives (Ends)
Inform
Line of Business Action Plans (Mission)
Refined into
Strategies and Tactics (Means)
Account for
Line of Business Influencers
Hinder or assist
Opportunities, Threats, Strength and Weakness
Can be determined through
Line of Business Assessment
Influences
Business policies and Business rules
Govern & Guide
Courses of Action
(Other policies, Regulations, programs, Business functions and processes, projects, schemes etc)

Figure 16.0: Business Building blocks

Recommendation

Using the Business Reference Model:

Create Efficient Government Business Environment: The BRM is designed to provide public institutions with a standard means to categorize their capital investments, identify areas for collaboration, consolidation and reuse based on the business their mandates/functions are being delivered, and help improve the overall IT architecture to better enable strategic outcomes.
FEAF creates BRM to benefit the public institutions at all organizational levels, from CEOs to developers.

CEOs and Directors: The BRM enables CEOs and directors to see the gaps and redundancies within their organization. These gaps and redundancies are opportunities for cost savings and new business capabilities that help achieve the organization's strategic objectives.

ICT Directors/Head: The use of the BRM as a framework for IT portfolio management ensures proper alignment of IT projects and investments to the business needs of the organization. It also helps guide the development of business cases to request and justify funding for future development and maintenance of IT programs, systems, and applications.

IT Project Managers: During the concept and planning phase of a project, the BRM allows project managers to identify current business capabilities and determine if or how the proposed project fits into the existing architecture. Project managers can also use the BRM to streamline common business processes to reduce or avoid cost, improve cycle time, and improve customer satisfaction and value. Additionally, application performance may be enhanced by finding better ways of doing business.

IT Project Developers: From a development perspective, the BRM enhances the ability for project teams to work towards a common, shareable solution for satisfying business needs. The costs associated with maintaining duplicative applications and services can be reduced by developing sharable services that can be used by more than one application or organization. Integrated service delivery approaches can also reduce the burden on the public by collecting data once and sharing it among systems, thereby reducing the burden on users of those systems.

Public institutions are advised to:

1. Promote policies that ensure categories of government operations in business areas are properly **enabled by Information technology** by thoughtfully following the principles of the WoG Operating Model (WOM), the **enterprise architecture reference model** and ensure IT is governed through the **IT engagement model**.

2. Ensure that **IT is driven and properly aligned** with every **building block of the business reference model**. IT should be a strategic tool for implementing all the building blocks especially **strategies** and **tactics** to enable **efficient public service delivery**.
3. Adopt business analysis and development standards and approaches such as business process modelling (**Business Process Modeling -BPMN**, **Unified Modeling Language-UML**, **Business Process Execution Language-BPEL** etc.)
4. Set performance objectives (especially for IT initiatives) and use the method in Performance Reference Model (PRM) to evaluate and measure IT performance against business goals and objectives.

3.2.2 Service Reference Model

Introduction and Purpose: The Service Reference Model (SRM) is a framework for defining, transforming, delivering and measuring the services provided by the public institutions in fulfilment of their mandates and functions. A line of business is created and mandated to deliver certain public services statutorily. The delivery of these public services is enabled by business processes that are defined and tailored to achieving a line of business objectives. At the heart of BRM is service.

The SRM is a business-driven, functional framework classifying Service Components with respect to how they support business and performance objectives. It serves to identify and classify Service Components that support Public Institutions and their IT investments and assets.

The purpose of SRM is to:

1. Encourage public institutions create services in line with their mandates/functions;
2. Provide a framework for public service discovery, definition, transformation and delivery; and
3. Provide tools and recommendations for integrated (cross-portfolio) service provision.

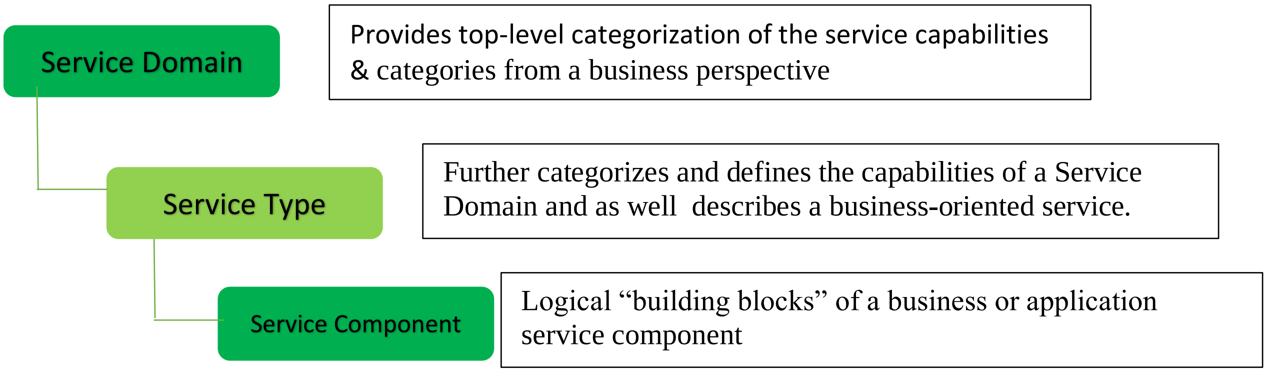
NGEA High-Level Expectation of Service Reference Model: The following highlights at high-level what is expected of SRM. This expectations are the outcome of SRM and what each public institution and national IT governing structure must work to achieve as each IT project is being added to the enterprise (Nigeria).

1. ***Alignment of Service with Statutory Functions/Mandates***: SRM provides for autonomy of public institutions to define services that best represents their statutory functions/mandates. However, the control should be based on public institutions' alignment of service provision to statutory mandates/functions;
2. ***Customer-centric and Customer-driven Digital Services***: Digital services provided by public institutions should be customer-centered and driven. SRM emphasizes major stakeholders' (Citizen, Business & Government) engagement and high consideration in service design and implementation.
3. ***Integrated Service Delivery***: Cross-portfolio services (involve two or more public institutions with disparate mandates) call for integrated service delivery to save cost, improve service access and convenience. This approach is termed one-stop shop, single-window, join-up government etc. and it requires two or more MDAs'

business processes to deliver service through a single channel seamlessly and at an affordable cost, using ICT. The channel can be multiple, but the same experience across different channels should be felt by customers.

The SRM Abstract Model

The FEAF structure of the Service Reference Model is composed of hierarchical structure that includes **Service Domains**, **Service Types**, and **Service Components**. This model aids in recommending service capabilities to support the reuse of business components and services across the public institutions.



Provides top-level categorization of the service capabilities & categories from a business perspective

Further categorizes and defines the capabilities of a Service Domain and as well describes a business-oriented service.

Logical “building blocks” of a business or application service component

Figure 17.0: The SRM Abstract Model

Service Domain: FEAF defines seven (7) Service Domains. Service Domains provide a high-level view of the services and capabilities that support enterprise and organizational processes and applications. They are differentiated by the business-oriented capability they represent.

1. Customer Services
2. Process Automation
3. Business Management Services
4. Digital Asset Services
5. Business Analytical Services
6. Back Office Services
7. Support Services

Service Types: As defined by FEAF the seven Service Domains are comprised of Twenty Nine (**29)** Service Types that further categorize and define the capabilities of a Service Domain. The Service Types define the second level of detail that describe a business-oriented service. Some of the examples are Customer Relationship Management

(CRM), Tracking and workflow, Supply Chain Management, Document Management, Business Intelligence, Human Resources, Security Management etc.

***Service Components**:* The next and final layer of the SRM is the Component level. It includes one or more **services** or **components** that provide the "**building blocks'** to deliver the information management capability to the business. A Component is defined as "a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface. The FEAF specified **168** well-known Service Components that can be created, used and reused across public institutions. Some examples of them are: Call center management, process tracking, inventory management, Document imaging and OCR, Decision Support and Planning, Recruiting, Identification and authentication etc.

The Tables A.1 in the appendix indicates 168 well-known service components

Note: These are general service domains that are likely associated with public institutions' business sub-functions and can form the foundation for reuse of applications, application capabilities, components, and business services. To provide statutory services, public institutions can create and define their own services domains, types and components separately from those defined in the FEAF.

Creating and Defining Services

To specify and create services that are distinct to each public institution and use by others, those services must be defined. The **definition** of services leads to their **transformation**, **delivery** and **measurement** vis-à-vis Performance Reference Model.

The conceptual model for specifying services are indicated in figure 18.0.

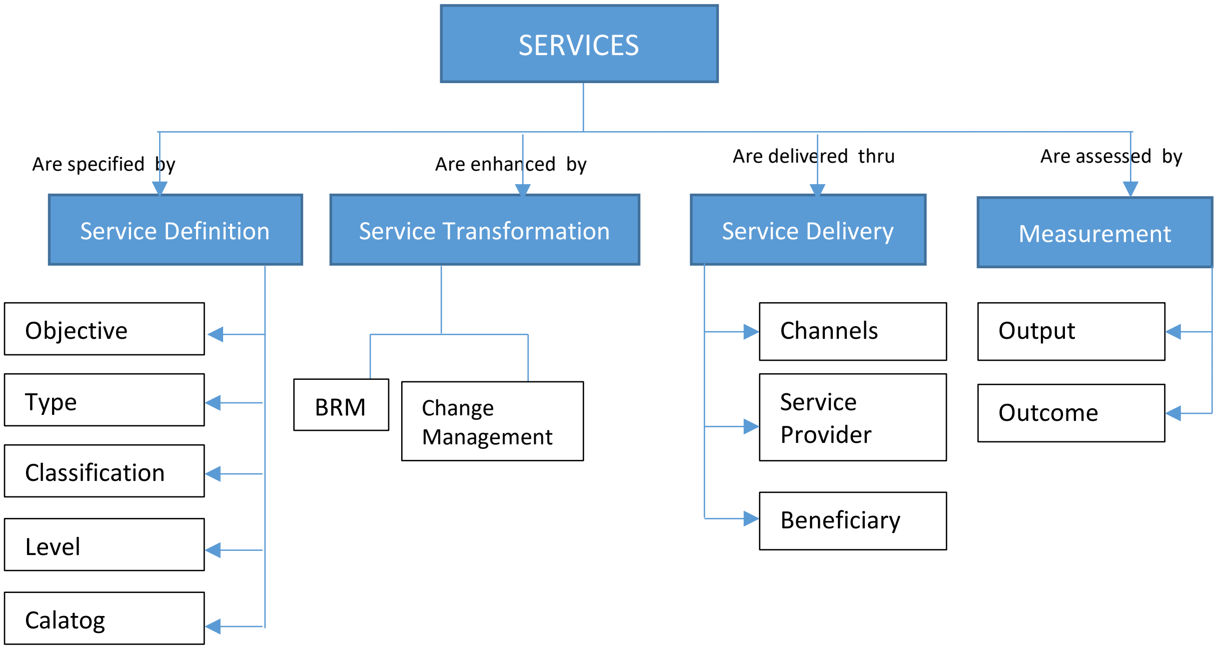


Figure 18.0: Service definition reference model

Service Definition: Service definition specifies components needed to describe the service by public institutions. It seeks to capture all the attributes of a Service included in the Service catalog. It comprises of the following:

Objective: Defines what to be achieved with service. The objective must be specific, measurable, actionable, realistic and time bound.

Type: Service type describes the kind of service to be offered and delivered. It is a categorization based on the interface between the Government and the customer. NGEA, asides from the service type defined in the FEAF, defines types of Services provided by the government to customers as:

1. Government to Citizens (G2C)
2. Government to Business (G2B)
3. Government to Government (G2G)

Service Classification: it categories services based on their tendency for reuse across public institutions. This leads to cost effectiveness and faster time-to-delivery. In actual practice, no two services of the legacy systems are identical. They perform at least slightly different function. However, it is necessary to group the services on 'approximate similarity' and then identify the sets of services which can be replaced by a single service as suggested by Ne-GIF, based on the greatest common requirements of the older services being replaced.

The Classification of Services based on level of reuse is listed as follows:

1. ***Core Services***: These are kind of services that are usually and supposed to be used by all public institutions They are domain-agnostic. Examples are: Government domain (.gov.ng), e-mail services and messaging services.
2. ***Common Services***: These kind of services are usually governed by government rules and regulations and used in the same manner by all the public institutions. Examples are HR (IPPIS), Finance (GIFMIS and TSA) etc.
3. ***Cross-portfolio Services:*** These services are provided by two or more of public institutions but not all. They are delivered through a single window or platform as an integrated service such that a single workflow cuts across multiple departments and providing the end result to the customer as a final response. e.g. Single Window Trade, One-stop Shop Investment program, social benefits, educational services, economic assistance services, etc. This improves access and fasten response to government services without government customers necessarily have to go to many government organizations for approval. The Ne-GIF provides steps for achieving this proposition.
4. ***Organization-Specific***: These are public institution-specific services that are provided/ utilized by one and only one government organization.

Note: For cross portfolio services, the processes and steps required are defined in the Ne-GIF document.

Service Level: Service Level is the **timeline** within which a service has to be delivered by the agency responsible for it. **Servicom** mandates all public institutions to publish Citizen Charters to notify the service levels to which they are committed. Public institutions are also required to sign **Service Level Agreements** with the private service providers to back up their commitment to the customers.

Service Catalog: Every public institution is expected to catalog its digital services. As part of NGEA implementation NITDA will provide directory of all digital services in FPIs. The benefits are:

1. It helps to identify common services that can be built once and used in multiple contexts;
2. It helps in planning for the interoperability and integration of the services in a more optimized fashion; and
3. It reduces overlap and duplication of services,

Service Transformation**:** To improve service delivery, it should undergo a service transformation: The following guidance is provided:

Business Process Reengineering (BRM): Public institutions are expected to use best practices to BRM methodology to carry business process reengineering. The BRM should eliminate unnecessary delay and overheads in business process leading to effective digital service delivery.

The process forms the basis of the design of the Application Architecture at the level of Application Reference Model.

Change Management: Change management ensures expected outcome is achieved. It controls the process for updates or modifications to the existing business processes of an organization.

NOTE: All public institutions are advised to institute best practice change management methodologies/approaches to manage change in business process for a service delivery.

Service Delivery: For a transformed public service to be delivered effectively, factors such as appropriate channels, service providers and the beneficiaries must be factored into service delivery design and implementation. Therefore, Each public institution is expected to develop its **service delivery policy or strategy** that considers these factors. These factors are discussed as follows:

Service providers: To deliver a service, most times there is a need for a public institution to collaborate with sister organization(s) and/or private business along the service delivery value chain. These service provider partners should be identified, assessed and ensure there is **Service Level Agreement (SLA)** signed.

Service beneficiaries: Knowing the service beneficiaries helps in designing a workable delivery strategy. The beneficiaries are the reason why the service is created and are the most important stakeholders in public service delivery. Adequate engagement with beneficiaries is necessary to get their inputs, feedbacks and support and in turn makes delivery of service satisfactory and sustainable.

***Channel**:* The delivery of a transformed service should be through variety of appropriate channels suitable for each target customer groups. Availability of varieties of **digital service delivery channels** has transformed delivery of public service across the world. They have proved to be cost efficient, convenient, transparent and satisfactory to both customers and public institutions who provide the service. Each public institution is expected to develop its **digital service delivery channel strategy** that makes service accessible to the target customer groups at affordable cost, transparent manner and in most convenient way.

***Service Performance**:* Creating services and deploying infrastructure to run them is actually the easy part. Successfully getting users to consume those services in a reliable manner while supporting continuous change is the hard part. In order to achieve reasonable performance measurement both in terms of service efficiency and utilization having accomplished all that have been discussed about service, appropriate mechanisms must be put in place to guarantee proper **service governance, quality and management**. Part of these are also discussed at the Performance Reference Model. Two major factors that need to be considered are:

Service Output: Service output are the immediate product and/or public need offered or supplied to service beneficiaries. It is the supply or product of a service creation. Usually, service output is measured in numbers. E.g. 90% of tax payers have access to online tax payment platforms. It needs to be measured.

Service Outcome: Service outcome is the effect or change that occurred because of the service offered to service beneficiaries. Measuring outcomes requires a more significant commitment of time and resources. Service performance in terms of outcome has to be tracked over time.

Recommendations:

Using the Service Reference Model

Identify opportunities to share services government-wide: Ne-GIF encourages and provides steps for identifying projects, investments and services that drive collaborations, support for common business purpose and reuse of shared services to provide cross-portfolio services government-wide.

Each public institution are expected to create service charter for every service it delivers with **service definition** as a major component.

Service definition Template

Table 5.0: Service definition template

<table>
<tr><th colspan="10">Service</th></tr>
<tr><th colspan="10">Goal</th></tr>
<tr><th colspan="10">Sector</th></tr>
<tr><th colspan="10">MDA/Public Institution</th></tr>
<tr><td>Service Objective</td><td>Service Type</td><td>Service Classification</td><td>Service Level</td><td>Service Priority</td><td>Service Provider</td><td>Channel of Delivery</td><td>Beneficiary</td><td>SLA</td><td>KPI</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

3.2.3 Data Reference (DRM) Model

Introduction and Purpose: Data is core to the public institutions' businesses and services they provide. Public service delivery including digital services cannot be rendered in the most efficient manner without data in the proper structure and format.

Additionally, a whole lot of value is provided when data can be shared within or across Public Institutions. It gives them a better contextual view of their own internally generated data and common view of government-wide or citizens' data amongst other benefits. Efficient e-Services provision is hinged on the degree of citizens' identity data harmonization.

The primary purpose of DRM is to:

1. Promote the common identification, use, reuse and appropriate sharing of data/information across the federal government via the standard description and discovery of common data and the promotion of uniform data management practices.

NGEA High-level Expectation of Data Reference Model: The following highlights at high-level what is expected of DRM. These expectations are what each public institution and national IT governing structure must work to achieve as each IT project is being added to the enterprise (Nigeria).

1. ***Seamless Government-wide Data Sharing and Exchange***: The major expectation of the DRM is to ensure government data can be shared and also exchanged seamlessly within and cross public institutions. The implication of this is that it is expected of DRM to provide mechanism for making data available in a standardized format and through standard interfaces that make exchange and sharing seamless. This is necessary for making extraction of transaction data from disparate government applications easy and available to business processes necessary for public service delivery. It also enables common view of public data and information by ensuring transparency of silo systems.
2. ***Making Government Data Available for Digital Services***: Once the data is provided in standardized format and through standard interfaces, it is expected of public institutions to provide processes that make government data available for use to provide digital services including data security.

The DRM Abstract Model

The main purpose is to enable the common\uniform and consistent definition, identification, discovery, use, and appropriate sharing of data/information across public institutions and with its partners. The DRM provides recommendations on standards, tools and technologies that can be used at data architecture layer by the enterprise/solution/data architects who are supporting the Public Institution(s) in building an effective Data Architecture.

It also provides a standard means by which data may be described, categorized, structured and shared to facilitate the discovery and exchange of core data/information across the Federal government and its partners. Information sharing is enabled through the common categorization and structure of data. By understanding the business context of data, public institutions can communicate more accurately about the content and purpose of the data they require. The accuracy of the content and purpose of data improves government-wide information sharing capabilities.

To achieve the above, DRM is specified in three areas:

1. Data Categorization;
2. Data Structure/Description; and
3. Data Exchange.

The three areas deal with Discovery, Creation, Management and Sharing\Exchange of enterprise data. Database Schema, Data Steward and Exchange Package are the key concepts/ components in the 3 areas respectively. Defining Metadata and Data Standards are key activities in the design of Enterprise Data Architecture.

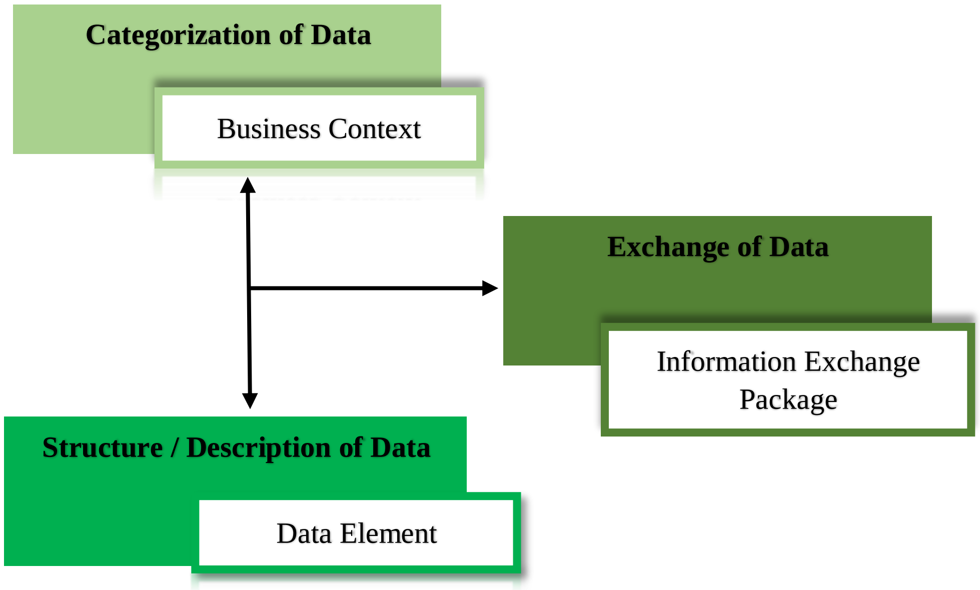


Figure 19.0:Abstract Model for Data Reference Model

Data Categorization: It establishes a ***Business Context,*** an approach through which agencies would be able to categorise data. This approach represents the business use of a given set of data and makes use of the ***Subject Area*** and ***Super Type*** to further describe the business context of a given set of data.

<u>Subject areas</u> represent a high-level set of business functions and are obtained from the Business Reference Model (BRM) discussed in the earlier section of this document.

<u>Super types</u> represent an additional level of definition of the business context and are generally related to specific business activities and/or processes that support the subject area.

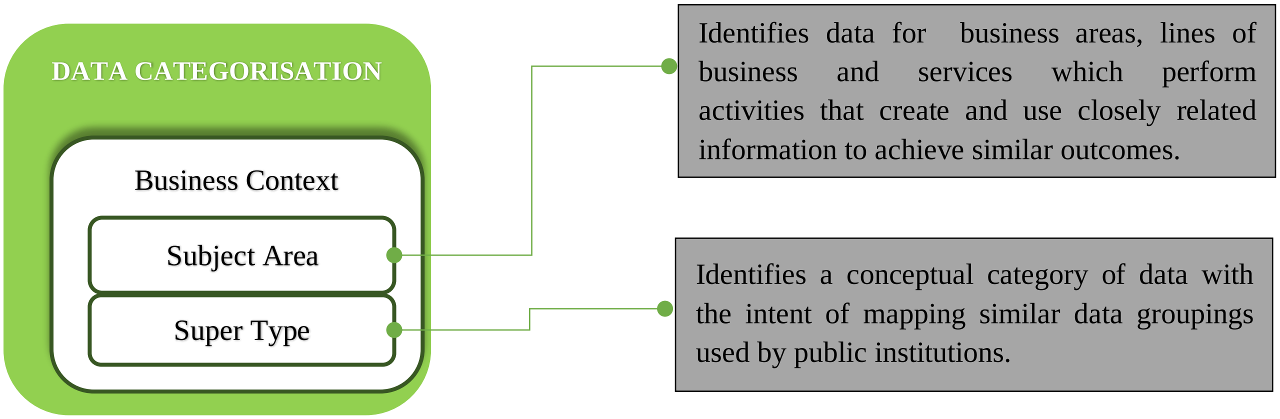

DATA CATEGORISATION
Business Context
Subject Area
Super Type
Identifies data for business areas, lines of business and services which perform activities that create and use closely related information to achieve similar outcomes.
Identifies a conceptual category of data with the intent of mapping similar data groupings used by public institutions.

Figure 20.0: Data categorization of the data reference model

Recommendation: Data categorization can be achieved through steps and recommendations highlighted in Nigeria e-Government Interoperability Framework (Ne-GIF) in the organizational and semantic interoperability levels.

Structure/Description of Data: Data Description provides a means to uniformly describe data, thereby supporting its discovery and sharing. Traditionally, data description was solely focused on organizing and describing structured data. With unstructured data as the largest focus of government's data management challenges around the world, the DRM Description component is being extended to focus on the larger topic of metadata, which includes both traditional structured data and unstructured data description.

Structure of data is described by the use of Data Element. This element consists of three data elements, which are adapted from the ISO/IEC 11179 standard. ISO/IEC 11179 **Standard describes the metadata** and activities needed to manage data elements in a registry to create a common understanding of data across organizational elements and between organizations. These elements are:

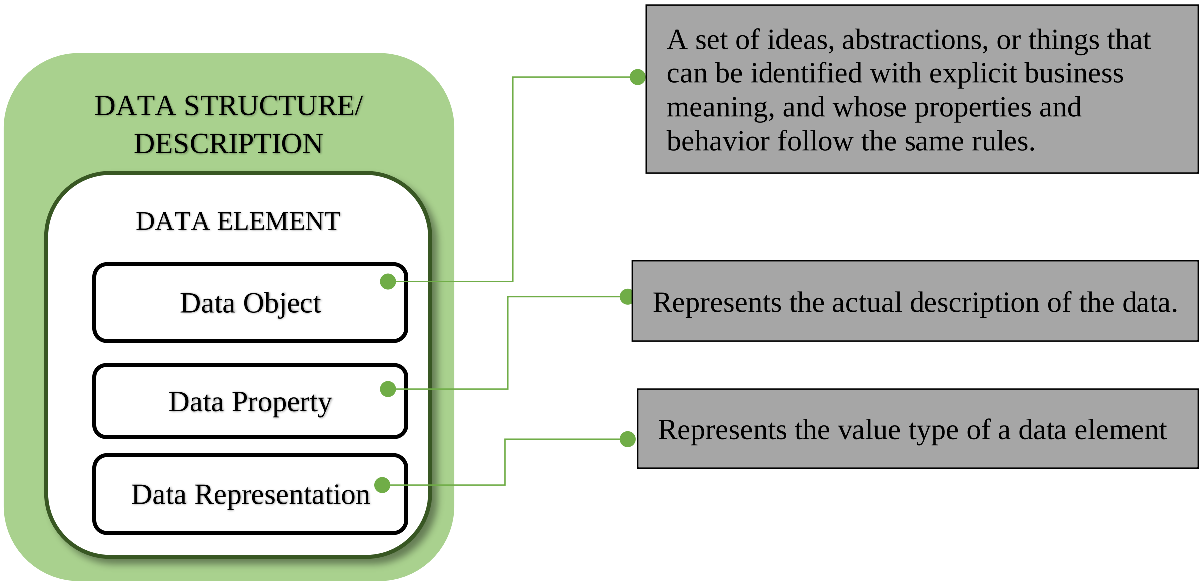

DATA STRUCTURE/ DESCRIPTION
DATA ELEMENT
Data Object
Data Property
Data Representation
A set of ideas, abstractions, or things that can be identified with explicit business meaning, and whose properties and behavior follow the same rules.
Represents the actual description of the data.
Represents the value type of a data element

Figure 21.0: Data structure or description of the data reference model

Recommendation: Data structure or representation can be achieved through steps and recommendations highlighted in Ne-GIF in section on semantic and technical levels of interoperability.

Exchange of Data: Data exchange can be executed through the DRM's information exchange package concept.

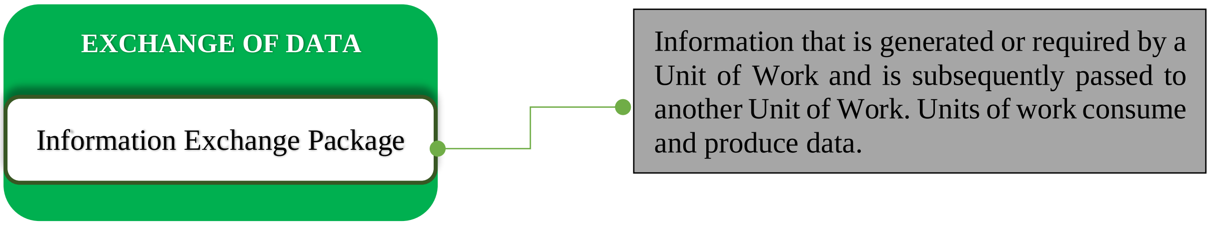

EXCHANGE OF DATA
Information Exchange Package
Information that is generated or required by a Unit of Work and is subsequently passed to another Unit of Work. Units of work consume and produce data.

Figure 22.0: Data exchange of the data reference model

The ***Information Exchange Package*** represents the actual message or combination of data that is exchanged between users of the data. The information exchange package brings the business context and data element (described in the structure of data section) together to define how a common transaction (the exchange of information and data) might appear. The package assists government, public organizations and other stakeholders to properly define how to exchange information for reuse. Information exchange package represents a specific business purpose. It makes use of the ISO/IEC 11179 concept of Information Interchange. The illustration of the data exchange is shown in the diagram.

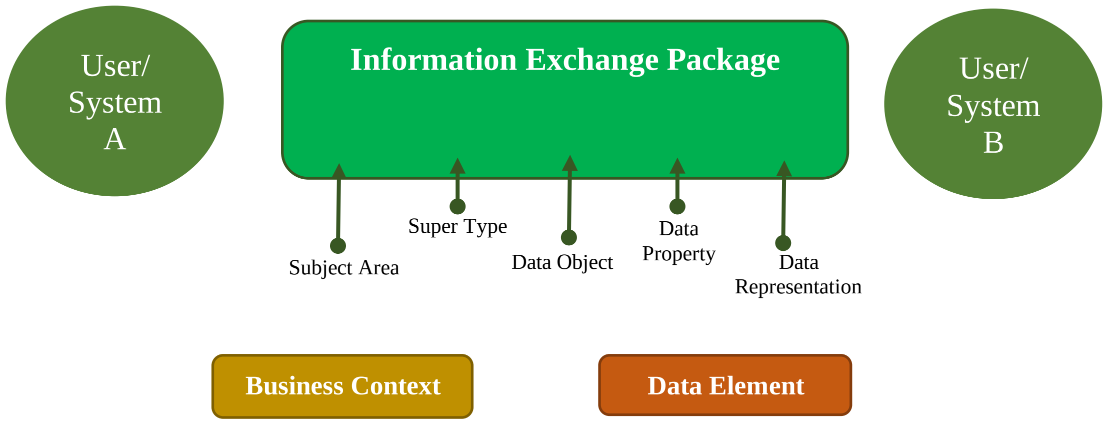
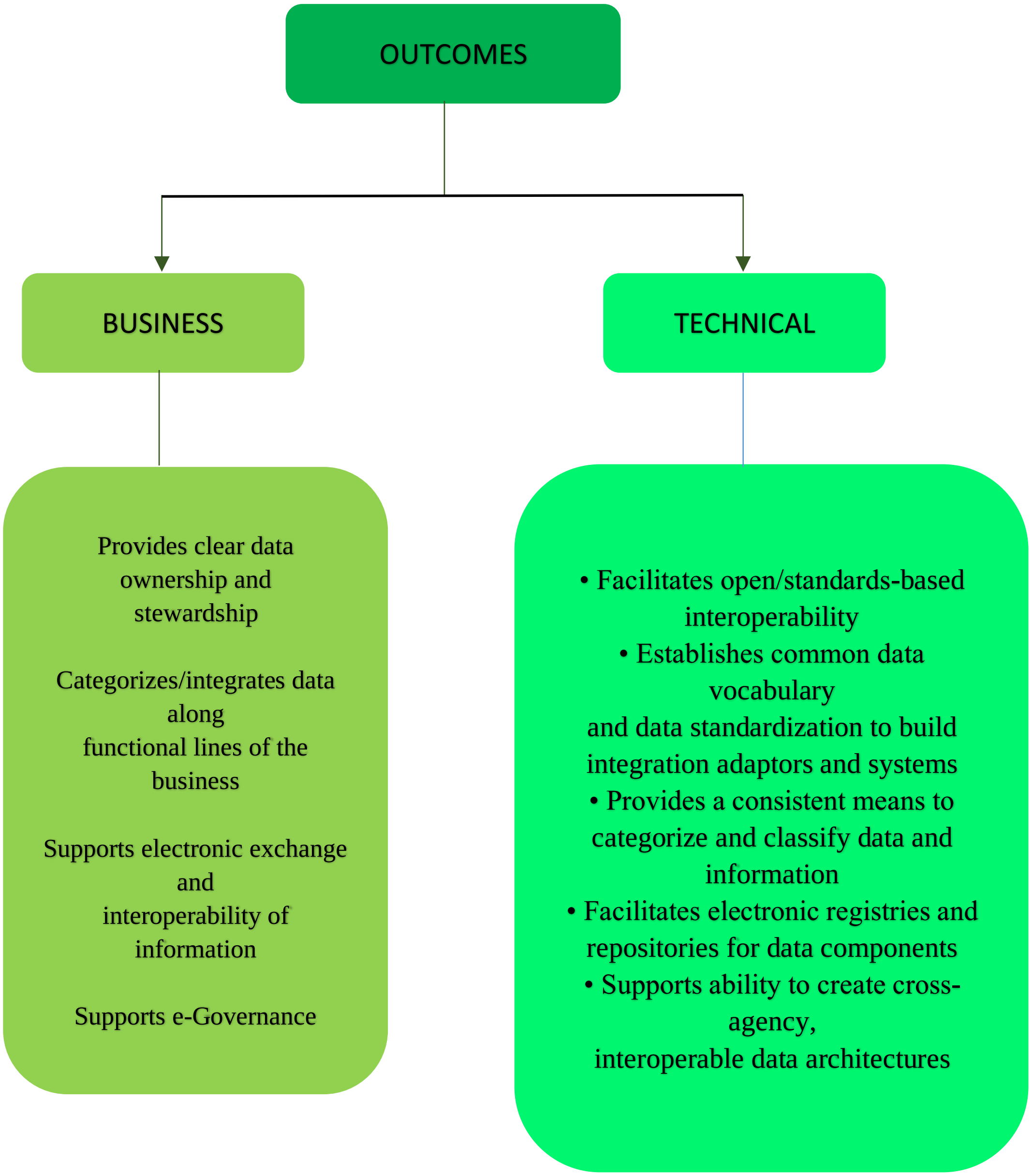


Figure 23.0: Information exchange package

Recommendation: It is recommended that the provisions, steps, tools, specifications, standards and recommendations in chapter three of Ne-GIF is properly adhered and followed to ensure seamless information exchange across public institutions.

Outcome Of Data Reference Model**:** The outcomes of the Data Reference Model (DRM) could be business or technical as illustrated in the chart.



OUTCOMES

BUSINESS

TECHNICAL

Provides clear data ownership and stewardship

Categorizes/integrates data along functional lines of the business

Supports electronic exchange and interoperability of information

Supports e-Governance

- Facilitates open/standards-based interoperability
- Establishes common data vocabulary and data standardization to build integration adaptors and systems
- Provides a consistent means to categorize and classify data and information
- Facilitates electronic registries and repositories for data components
- Supports ability to create cross-agency, interoperable data architectures

Figure 24.0: Data Reference model outcome

Recommendations

Using the Data Reference Model

Providing Standardized Information Exchange: This is to facilitate a standardized information exchange across a Community of Interest. Creating a standardized information exchange with agreed upon data descriptions enables each participating organization to create the necessary interface to receive or provide data only once. Existing exchange partners can use a new participant's data without having to write any interface or transformation. Also, it improves the quality of information exchange by ensuring that the source and target mapping is accurate, through the exchange model and standardized data definitions.

Method: Model the exchange and build exchange schemas using available data standards. Ne-GIF recommends approaches and steps for data exchange in the section on levels of interoperability

Best Practices

The DRM describes data and information needed to perform business and mission functions of government by use of collective methods. The three fundamental method areas associated with the DRM to help public institutions consistently categorize, describe, and share their data are: Data Description, Data Context, and Data Sharing as explained in the DRM abstract model.

Data Description: The methods listed below explain best practice examples meant to inform and enhance public institutions' data description processes and to align their data practices with the FEA DRM.

1. Integration Definition for Function Modeling (IDEF). The model IDEF1X is used to define a logical data model when the target deployment is known to be a relational database. www.itl.nist.gov/fipspubs/idef1x.doc
2. The Open Government Group Architecture Framework (TOGAF). TOGAF® defines an Architecture Development Method (ADM) that uses the four business, application, data, and technical architecture domains. http://www.opengroup.org/togaf
3. Unified Modeling Language™ (UML). UML is a mature and widely adopted technology- independent, modeling language that supports the application development life cycle. http://www.omg.org/spec/UML/
4. Department of Defense Architecture Framework v2.02 (DoDAF v2.02). The DoDAF v2.02 provides detailed guidance for "fit-for-purpose" architecture development. http://dodcio.defense.gov/sites/dodaf20/
5. ISO/IEC 11179. An international standard that specifies the kind and quality of metadata needed to describe data and that specifies how to manage metadata in a metadata registry. http://www.iso.org/iso/home.htm
6. Dublin Core. A core metadata vocabulary

Data Categorization (Context): The methods listed below explain best practice examples that can be used by public institutions to categorize its data and align their data practices with the FEA DRM.

1. ***Data Asset Catalog***. An agency can create a data catalog with the following steps:

a. Inventory data assets and collect the data model or structure for each asset;
b. Map the asset characteristics to the DRM Taxonomy; and
c. Preserve the results in a data catalog.

A data asset catalog reduces time and cost to implement change by reducing the time to locate needed data, identifying redundant data assets for decommissioning, and identifying opportunities to reuse or extend a data asset rather than creating a new data asset. The data asset catalog also provides the foundation of an enterprise data inventory, which lists and describes public institution's data sets used in the its information systems.

2. ***Information Discovery and Search***. By mapping each data asset in the agency's data asset catalog to the agency's data categorization taxonomy, an agency can enable users to discover the information they need without having to know in advance where it is or even if the particular information exists. The discovery and search capability uses the data categorization taxonomy to identify the data assets that satisfy the search criteria of the user.

Data Sharing (exchange): Data Sharing is the use of information by one or more consumers that is produced by another source other than the consumer. It supports the access and exchange of data and is enabled by capabilities provided by both the Data Context and Data Description standardization areas.

The methods listed below describe the best practices used for information sharing. This guidance is meant to inform and enhance effective agency information sharing processes.

1. ***Linked Data, or Linked Open Data (LOD)***. The Web enables the link of related documents and similarly it enables the link of related data. The term Linked Data, or Linked Open Data (LOD) refers to a set of best practices for publishing and connecting structured data on the Web. Key technologies that support Linked Data are URIs (a generic means to identify entities or concepts on the Web), HTTP (a simple yet universal mechanism for retrieving resources, or descriptions of resources on the Web), and RDF (a generic graph-based data model with which to structure and link data that describes things on the Web). See http://linkeddata.org/home.
2. ***Nigeria e-Government Interoperability Framework (Ne-GIF)***: It provides tools, specifications and guidelines for supporting MDAs/Public Institutions in undertaking data and e-Government interoperability.

3.2.4 Application Reference Model (ARM)

One of the major objectives of e-government is to automate government services through information systems. Effective automation of public services requires applications that digitize **government processes and data** within and/or across public institutions. By automating government services through applications, better services can be provided to government customers. It provides the foundation to automate these Services.

The ARM is a categorization of different types of software, components and interfaces. It includes software that supports or may be customized to support business. It does not include operating systems or software that is used to operate hardware (e.g. firmware) because these are contained in the IT Infrastructure Reference Model.

Applications are defined as logical groups of capabilities that manage and process the data objects in the DRM, support the business functions in the BRM and power the services defined in SRM. In NGEA, applications and their capabilities are defined without reference to particular technologies. They are stable and relatively unchanged over time, whereas the technology used to implement them might change over time, based on appropriate technological trends currently available and the change in business needs.

The ARM main purpose is to provide framework for adopting applications for automating government business processes and services, maximize re-use of core/common applications and define categories of major application systems necessary to digitize government data. Additionally, a whole lot of value is provided when public institutions can share and integrate application services amongst themselves, giving them a chance at providing one-stop shop services to their stakeholders.

NGEA High-level Expectation for Application Reference Model: The following is expected to be achieved at the application layer of the reference model.

Core/Common Applications Interoperability and Organization-specific Applications Standardization: The Coordination Operating Model strongly promotes high requirements for core/common/cross-portfolio applications interoperability/ and integration but low institution-specific applications standardization.

The implication of this is that, at the application layer of the reference model, there is a strong need for core/common/cross-portfolio applications integration to meet WoG requirements for data sharing and exchange. On the other hand, low institution-specific application standardization means high level of control by public institutions to make decisions on the choice of domain-specific applications that are suitable for their operations and statutory mandates/functions' achievement.

The integration requirements will help public institutions eliminate applications redundancy, by finding opportunities to share, reuse or consolidate applications including their licenses and negotiate reduced pricing where necessary. In addition, cost reduction requirement will pave way for moving to open-source software for application development where necessary.

Note: The adoption of Coordination Operating Model enables public institutions to abide by the WoG requirements for Core/ Common/Cross-portfolio and Public-Institution Specific Data Elements, Processes and Applications. These requirements are to ensure seamless interoperability amongst applications, enable sharing and re-use of applications which in-turn, provide cost efficiency to the Government. Most importantly, the coordination operating model enables individual public institutions to have control over procurement/development of applications that meet their specific business needs and business processes.

Reduction in the Cost of Application Portfolio Management: ARM provides framework to encourage reuse of core/common Applications government-wide. Public institutions are expected to use ARM to promote core/common applications reuse through business process re-engineering concepts that identify common processes that can utilize existing applications across the government.

ARM Abstract Model

The ARM Abstract Model is specified through the following building blocks modeled in figure 25.0.

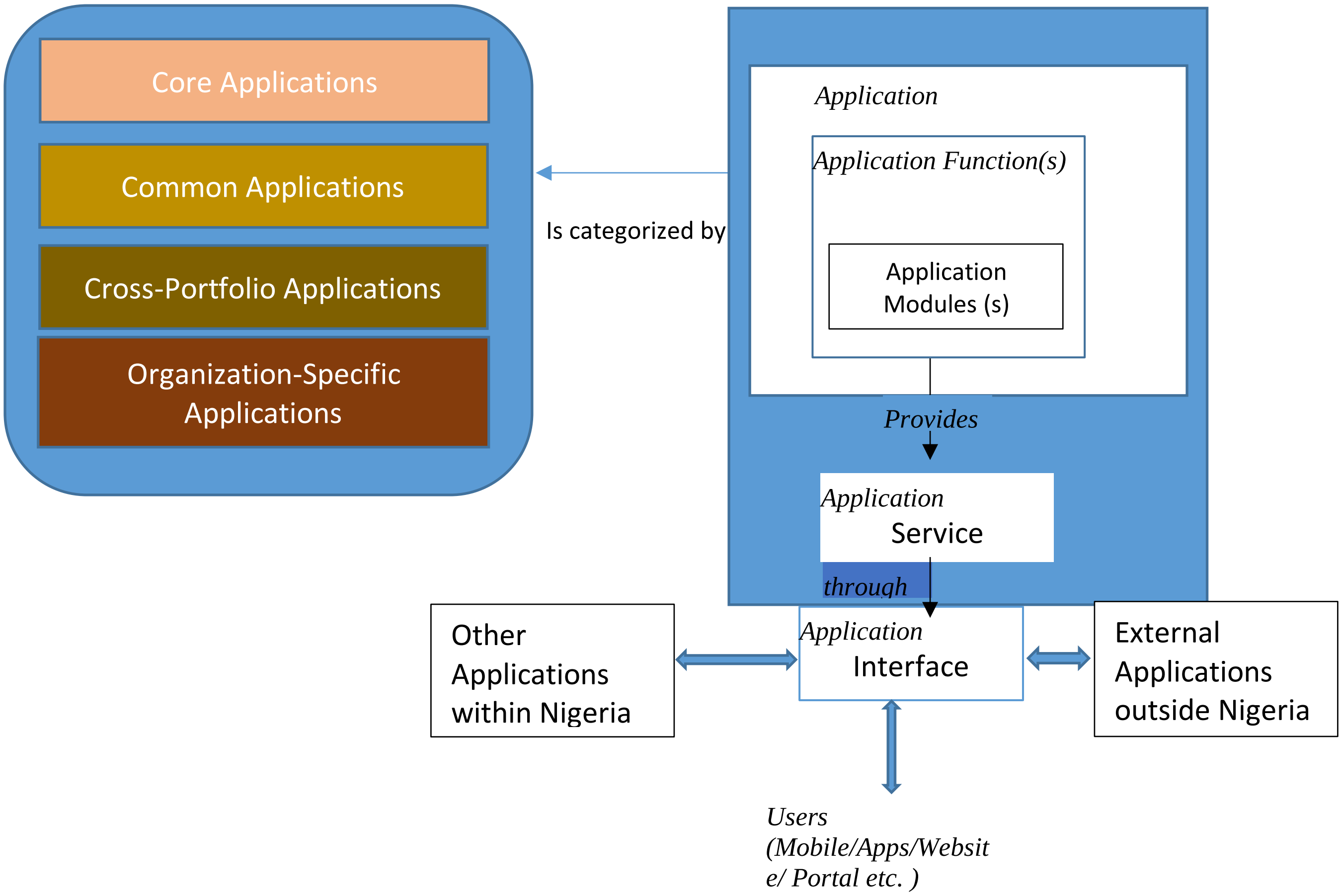

Core Applications
Common Applications
Cross-Portfolio Applications
Organization-Specific Applications
Is categorized by
Application
Application Function(s)
Application Modules (s)
Provides
Application Service
through
Application Interface
Other Applications within Nigeria
External Applications outside Nigeria
Users (Mobile/Apps/Website/ Portal etc.)

Figure 25.0: ARM Abstract Model

Application: Is a program or set of programs that consists of Modules/Sub-Modules/Functions, Input & Output Data Sources and Interfaces, developed by public institutions to automate their specific business processes and services in order to accomplish business functions/mandates. Typically, application consists of three levels:

Application Systems: Are discrete sets of information technology, data, and related resources, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information in support of a specific business process.

Application Components: Are self-contained software, which can be aggregated or configured to support, or contribute to achieving, many different business objectives. For example, workflow management, document management, records management and many other types of components can support multiple IT Systems and business processes.

Interfaces: are standards and protocols used to transfer information from one application system to another.

Figure 26.0 shows FEAF defined application reference model based on application system, components and standardized interfaces.

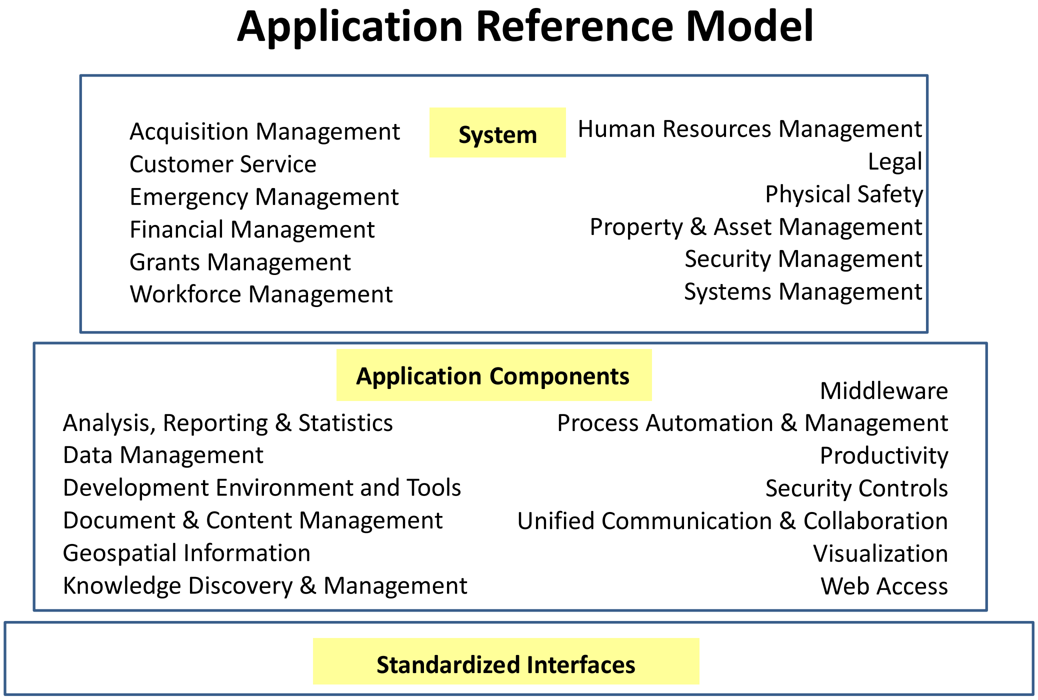


Figure 26.0: FEAF example of application reference model

Application Categorization

NGEA categorizes Application is categorized into **core, common, cross-portfolio and organization-specific applications** categories.

Core Applications: They form the foundation upon which common and organization-specific applications are driven. E.g. .Gov.ng Domain Registry, National Identity Database Management System, National Enterprise Middleware Services, National Digital Authentication Platform, National API Gateway etc.

***Common Applications*:** The common applications are those that are maintained centrally with functionalities required and shared by all public institutions to operate. e.g. IPPIS, GIFMIS, TSA, e-Procurement etc.

Cross-Portfolio Application: These are the applications that are designed and developed to deliver a single service or a set of related services in an organized manner by two or more public institutions in response to a single request. e.g. Single Window Trade Portal, One-stop Shop Investment Centre (OSIC) etc.

Organization-Specific: These are applications designed and developed by each public institution to carry out its mandates/functions. Each Public institution has the sole responsibility to propose domain-specific applications for their operations. This gives opportunities to public institutions to be autonomous and independent in carrying out their mandates/functions. e.g. taxation, Pension, tourism, public safety, Energy, Oil & Gas, Post Service etc.

Application Service: is a set of interconnected applications which are configured to offer a service to the organization. Application service automates government service(s). This increases productivity, responsiveness and efficiency on the part of the government. On the part of the government's customers, it improves service accessibility and convenience.

Application Function: Application function is the specific capability that the application provides to fulfill Application Service. Each Application is composed of one or more Modules & Sub-Modules. Each Module/ Sub-Module can provide one or more Functions. Business Services are fulfilled using one or more Functions. An application function is likened to an application system.

Application Modules: An Application Module is a logical container for coordinated objects related to a particular task, with optional programming logic. It is a class that represents a business application task. Specifically, it encapsulates the data model associated with a task, plus the custom code to implement the task. An application module is likened to an application component.

Application Interfaces are standards and protocols used to transfer information from one application system to another. They consist of system and user interfaces which promotes application and service access and as well as data exchange between applications.

The figure 27.0 depicts the NGEA application portfolio. It comprises of four layers in the ARM with examples of applications at each layer.

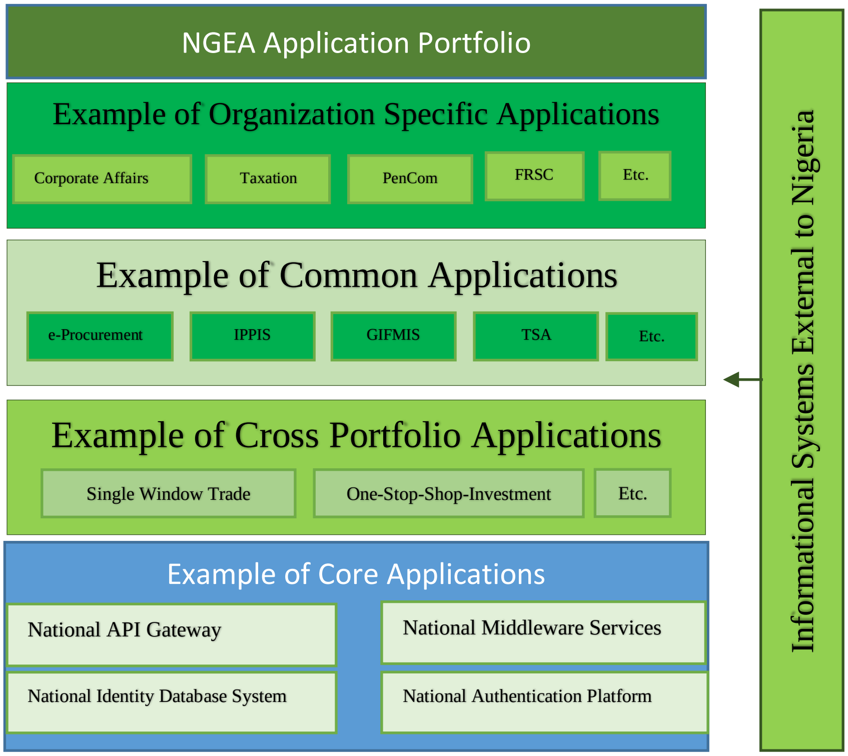

NGEA Application Portfolio
Example of Organization Specific Applications
Corporate Affairs
Taxation
PenCom
FRSC
Etc.
Example of Common Applications
e-Procurement
IPPIS
GIFMIS
TSA
Etc.
Example of Cross Portfolio Applications
Single Window Trade
One-Stop-Shop-Investment
Etc.
Example of Core Applications
National API Gateway
National Middleware Services
National Identity Database System
National Authentication Platform
Informational Systems External to Nigeria

Figure 27.0: NGEA Application Portfolio

This helps public institutions categorize applications according to need areas, make gaps and redundancies become evident and identify collaboration requirements between local and international stakeholders for efficient delivery of mandates/functions.

NOTE: The figure 27.0 is not an exhaustive portfolio of applications but rather an example of application portfolio in Nigeria and how they can be categorized.

Recommendation

Using the Application Reference Model (ARM)

IT Cost Reduction through IT/ Application Portfolio Management: The aim is to find opportunities to reduce the cost of business applications across government.

Method: This can be achieved by using ARM to map systems. This is to look for redundancy and find opportunities to share, reuse, or consolidate information systems; or to consolidate licenses and negotiate reduced pricing. There is a need to review the mappings from across the Federal Government, if they are available, to identify opportunities for sharing and reuse that span agencies. By mapping public institutions' systems and application components to the ARM, a digitized searchable dataset can be produced so that manual information gathering is not needed. This analysis may result in consolidating instances of the same application, consolidating licenses, selecting a WoG solution that will be hosted in the cloud, or even changing business processes to enable sharing.

Using ARM with the Other Six Reference Models: This ensures correct technologies/applications that meet a well understood business need are determined and best choices are made. By using the same taxonomies to map both project needs and existing solutions across the six reference models, extensive and comprehensive information can be searched easily to identify opportunities for reuse or sharing. Then the solution team, including the business owners, can use industry standard methods to perform an objective, data-driven analysis and determine whether an existing solution is a sufficiently good fit for the environment and purpose, and if so, which one.

Method: The architects supporting the public institution's efforts should work with the solution team (IT/ICT department team) to map the project elements to the other six reference models. Using this mapping, the architects use the repository of organizational and governmental reference models mappings (mapping of the other six reference models) to find systems, services and solutions that might meet such institution's needs.

Best Practices

The best practices as presented in FEAF have three emerging approaches that can be used in conjunction with each other to exploit the information in the implemented ARM (i.e. **the ARM structure** plus the **agency mapping of applications and investments** to it), as well as the other Reference Models. These methods are: **Capability Modeling and Analysis**; **Service Oriented Architecture**; and **Portfolio Management**. The use of the methods to solve enterprise problems allow sharing and re-use capabilities of the FEA Reference Models to be met. In addition, the three methods enable modularization and improve the flexibility of applications and the IT acquisition process.

a. ***Capability Modeling and Analysis***: Capability Modeling and Analysis is a Requirements Analysis technique that facilitates the translation of business/mission and technical requirements into discrete capabilities that lend themselves to sharing and reuse analysis (Shared-First). By casting requirements as capabilities at various levels of abstraction (meaning they may be decomposed into more detailed capabilities) and with **capability**

dependencies modeled, the **commonality across requirements is more obvious** than with standard requirements analysis or business process analysis techniques. Within the context of the FEA Reference Models, **capability requirements can be associated with elements and categories of the BRM for functional capabilities**, the **ARM for back-office and software support capabilities, and the IRM for infrastructure capabilities**. Capability Modeling and Analysis also has the advantage of modularizing the requirements so that capabilities can be combined in new ways to meet new business/mission and technical objectives. This method is a natural outgrowth of the Service Oriented Architecture (SOA) direction.

b. ***Service Oriented Architecture*****:** Service Oriented Architecture (SOA) is an architectural style in which IT solutions are assembled from a collection of interacting services. This method not only provides more application flexibility because services can be more easily modified or replaced, but also reduces the cost of developing and maintaining applications because the solution design is better understood and the impact of changes is isolated. The key to success with SOA is the development of an architecture of services – a layered diagram that depicts the services and their dependencies. This is critical in the consumption/reuse of services because it establishes the boundaries between services and indicates the relationships among them. Services can be mapped to the appropriate FEA Reference Models to assist in identifying candidate services for use in particular applications. For example, if a solution requires a document management service and/or customer relationship management service, the ARM will identify other applications that have this capability or services that can satisfy this requirements. Services contained in registries or repositories should be mapped to the ARM and other reference models to facilitate the discovery process.

c. ***Portfolio Management***: Portfolio management is widely applied to IT investments and programs. This method has significant benefits when applied to all IT assets – in particular services and applications. To promote reuse or sharing of services, portfolio management techniques should be used to assess assets for viability into the future and to develop a service lifecycle plan for each asset. For example, to continue the use of the document management application component and/or customer relationship management service, each existing (legacy or Commercial-of-the Shelf-COTS) document management component and customer relationship management component should be mapped to the ARM so that the reuse potential can be evaluated by potential consumers. However, if the legacy document management service is to be deprecated in the near future, this information should be associated with the service. In this way, potential consumers of the service will be informed of the lifecycle plans for the service. Portfolio Management techniques can also be used to support application functionality consolidation by analyzing the mappings to the ARM with the associated lifecycle information. In addition, this method may facilitate the analysis for shifting application components from legacy hosting to the Cloud Computing environment as well as the analysis for moving to open-source software.

3.2.5 Infrastructure Reference Model (IRM)

Introduction and Purpose: NGEA defines the IRM as specified in the FEAF version 2.0. IRM provides an abstract model for categorizing IT infrastructure, the facilities and network that host the IT infrastructure. It supports the definition of infrastructure technology items and best practice guidance to promote positive outcomes across information technology implementations.

The term infrastructure is defined in Enterprise Architecture EA as the generic (underlying) platform consisting of hardware, software and delivery platform upon which specific or customized capabilities (solutions, applications) may be deployed. Following the provisions of the IRM encourages sharing and reuse of infrastructure to reduce costs, increase interoperability across the government and its partners, supports efficient acquisition and deployment of IT infrastructure and enables greater access to information across WoG.

IRM does not only help in the categorization schema of IT infrastructure assets, it also helps public institutions in the analysis of IT infrastructure assets as well as assist the WoG in conducting Government-wide analysis of IT infrastructure assets and to identify consolidation initiatives. IRM is going be used by Public institutions to drive efficient IT infrastructure asset and management practices.

The shift in infrastructure acquisition and deployment moves at least three stages.

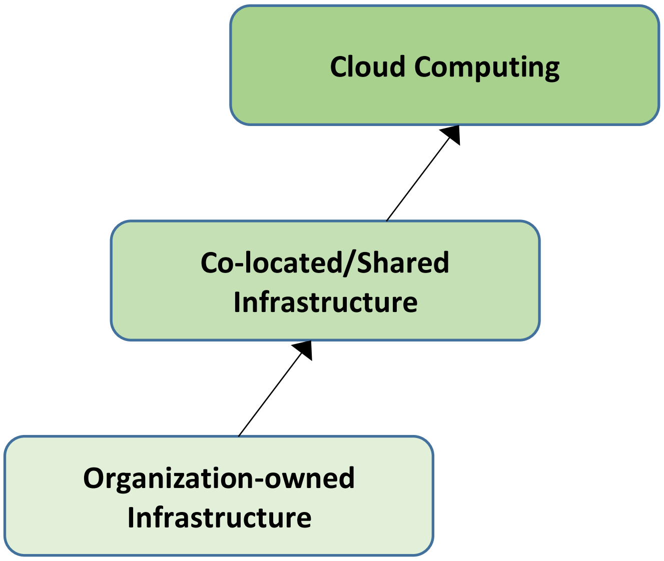

Cloud Computing
Co-located/Shared Infrastructure
Organization-owned Infrastructure

Figure 28.0: Infrastructure acquisition and deployment shift

Because of the tremendous economy of scale and scope as well as efficiency of IT environment benefits that could be realized by transitioning from one stage to another, governments have moved from stage one to stage two and many have transitioned to stage 3. Achieving standardized technology objectives might necessitate these transitions.

NGEA High-level Expectation of Infrastructure Reference Model: The following highlights exactly what is expected of IRM. The expectations are what government policies and regulations should address while deploying IT infrastructure.

Reduction in the Cost of Infrastructure Acquisition and Deployment*:* Reduction in the cost of infrastructure acquisition and deployment should be the focus at both organizational and WoG levels. This eliminates **duplication/redundancy** of IT infrastructure. In order to achieve this, there is a need to transition from organization-owned infrastructure drive to more of a co-located/shared infrastructure agenda with cloud computing as the final target.

Promote Shared Infrastructure/Services: Technology efficiency is gotten through the introduction of standardized and consolidated technology platforms as well as provision of shared infrastructure services. One of the greatest advantages or benefits of computing resources is their ability to be networked and virtualized. Networking and virtualization of computing resources greatly enables the idea of shared services. Shared services is the consolidation of IT infrastructure and back-office/business operations that are used by multiple public institutions. This does not only reduce the cost of infrastructure purchase by individual public institutions but also allow them to focus limited resources on activities that support their business mandates/goals. Shared infrastructure/services ensure that public institutions are free from on-going challenges of providing and managing IT services that are responsive to the ever-changing demands and needs of diverse business customers. The shared infrastructure/services providers is responsible for providing and managing the IT services.

Exception: There are exceptions that could prevent public institutions from going into co-location or cloud services (private or public cloud) options. Such exceptions are determined by IT Governance structure and waived by IT coordinating mechanism in the IT engagement model.

The IRM Abstract Model

NGEA adopts FEAF recommended structure for IRM. The structure is depicted in figure 29.0 below.

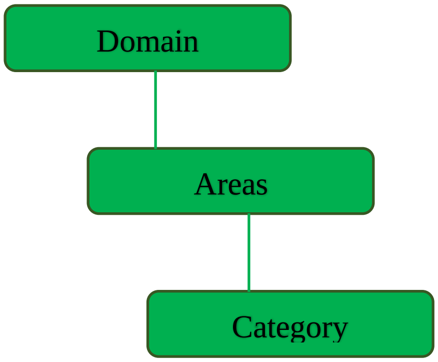


Figure 29.0: IRM Abstract Model

Domain: Domain is the level 1 in the hierarchy and it consists of three entities. They are Platform, Network and Facility, which are linked and related to each other to enable analysis of IT assets across the three dimensions.

Areas: Areas describes the level 2 of the hierarchy and it consists of 13 total Areas linked to the three Domains in Level 1.

Category: Category is the level 3 in the hierarchical structure that consists of many Categories as may be categorized by public institutions (for example, "Personal Computer – Laptop") and linked to the 13 Areas in Level 2.

NOTE: NGEA identifies 66 categories linked to the 13 areas.

For clarity and further explanation of the three domains, each domain is represented in a chart and explanation is presented in a table in Appendix A.2

Platform Domain: The Platform Domain includes a hardware architecture and a software framework, where the combination allows software, particularly application software, to run. For the purposes of the IRM, platforms include a computer's architecture, operating system, attached and internal devices, as well as software platforms that emulate entire hardware platforms (e.g., system virtualization).

Network Domain: The Network domain describes the Network section of the IRM and addresses how a particular IT asset accessed and used within the enterprise.

Facility Domain: The facility domain of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.

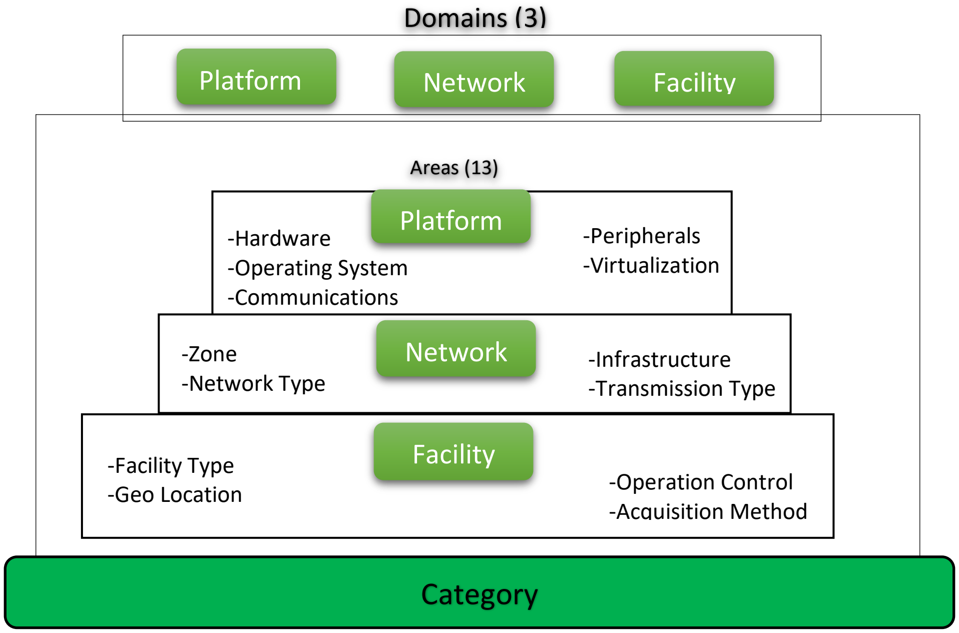


Figure 30.0: High-level IRM Taxonomy

Relationships Among the Domains The three domains of the IRM are linked and related to each other. The relationship enables analysis of IT assets across the three dimensions. These relationships are demonstrated in the figure 31.0.

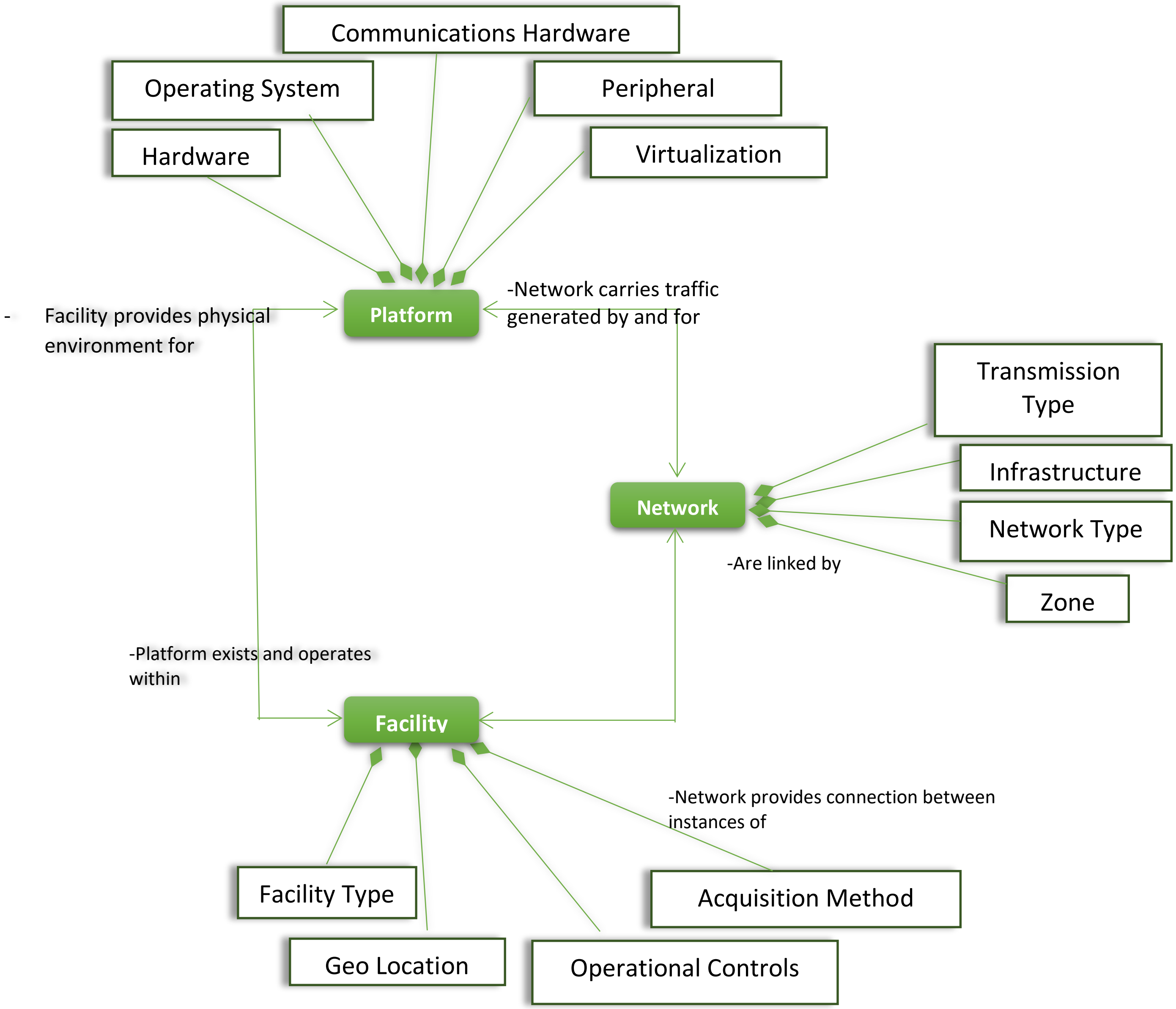


Figure 31.0: IRM Domain Relationship Model

Recommendations

Using the Infrastructure Reference Model

Fundamental to using the IRM as a decision making tool is an IT infrastructure asset inventory that is categorized using the IRM.

The IRM provides approach and categorization methods for:

1. Establishing and completing an IT asset management inventory;
2. Evaluating whether to consolidate infrastructure to the cloud, using the IT infrastructure asset inventory; and
3. Identifying opportunities for shared services

Method 1: By Mapping an organization's IT assets to the Infrastructure Reference Model (IRM), Business Reference Model and Application Reference Model (ARM) provides a robust technical definition for IT asset management inventory and insight into weather public institutions should continue with on-premise IT asset management or consolidation options (co-location/shared infrastructure and Cloud).

Method 2: Using the IT asset inventory and IRM categorization, public institutions could see a clear picture of duplicative infrastructure components and services in data centers that were owned and operated by them. Not only will this identify component services for internal private cloud implementation, due to security and information sensitivity requirements, but they also identify public cloud solutions that will sustain existing re-hosting and Operation & Maintenance needs while enabling a migration towards emerging technology and standards-based service model.

Best Practices

The following widely accepted best practices, guidance and standards can adopt IRM categorization as part of their implementation.

a. ***Control Objectives for Information and related Technology (COBIT)*** is an internationally accepted framework that provides an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises (i.e., COBIT helps to define what should be done). The principles, practices, analytical tools and models found in COBIT embody thought leadership and guidance from business, IT and governance experts around the world. COBIT is aligned with COSO, ITIL, ISO 27000, CMMI, TOGAF and PMBOK . The IRM is applied primarily in the Deliver and Support control domain.

b. ***Information Technology Infrastructure Library (ITIL) v3*** is the most widely accepted approach to IT Service Management in the world. ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally (i.e. ITIL helps provide the how for service management aspects). ITIL is aligned with various international quality standards including international standard ISO/IEC 20000 (IT Service Management Code of Practice).

c. ***Object Management Group (OMG)*** is an international, open membership, not-for-profit computer industry consortium with members worldwide, including government agencies, small and large IT users, vendors and research institutions. OMG is most known for their standards development work. Over time, OMG has evolved to meet the changing business needs of IT by playing a strong role as a builder of practitioner-driven Communities of Practice focused on Green/Sustainability, Service Oriented Architecture, BPM, Cyber Security and Event Processing, while staying true to its standards development roots.

d. ***NIST Cloud Computing Reference Architecture (CCRA) and Taxonomy (Tax)*** NIST SP 500-292 - communicates the components and offerings of cloud computing. Guiding principles for the creation of CCRA were that it had to be a vendor-neutral architecture that did not stifle innovation by defining a prescribed technical solution (i.e. the "how").

e. ***National Cloud Computing Policy:*** The Nigeria Cloud Computing Policy provides direction for cloud computing adoption in the public sector. It highlights cloud computing benefits, challenges (including privacy and security issues etc.), deployment models, expected outcomes of migration to the cloud, rational for adoption of "Cloud First Policy" among other things.

NOTE: Public Institutions and NGEA governance structure are advised to observe every provision of the IRM.

3.2.6 Security Reference Model (SecRM)

Introduction and Purpose: Security is an issue that cuts across all the reference models and all levels of public institutions. It forms the sub-architectures of the overarching EA across other reference models and enables security standards, policies, and norms to be developed and followed, since it is an enforcement point for Information Technology. The SecRM allows architects to classify or categorize security architecture at all scope levels of the NGEA reference model. An end-to-end security mechanism is a critical requirement at both system, organization, WoG levels respectively.

NGEA High-level Expectation of Security Reference Model: Data, as the life blood of digital services, is what passes through the fabric of Information Technology systems and since the public institutions depend on the information technology systems for their operations, then the security of both IT systems and data are crucial to their existence. The following highlights high-level expectations of the Security Reference Model.

Confidentiality, Integrity and Availability of Information System and Data: SecRM are expected to ensure protection of information system and data from **unauthorized access or disclosure**, **unauthorized modification** and ensuring their **availability anytime it is required**. **Authentication** (proving that a user is whom he or she claims to be) and **authorization** [the act of determining whether a particular user or computer system has the right to carry out a certain activity) are used to make information available to those who need it and who can be trusted with it. Thus, concepts relating to the people who use that information are authentication, authorization and **non-repudiation** (ensuring means of authentication cannot later be refuted - the user cannot later deny that he or she performed the activity). All these are expectations that must be fulfilled by the SecRM.

The SecRM Abstract Model

FEAF categorizes security reference model into three: Purpose, Risk, and Controls. The three areas are then divided into six total subareas as shown in figure 32.0

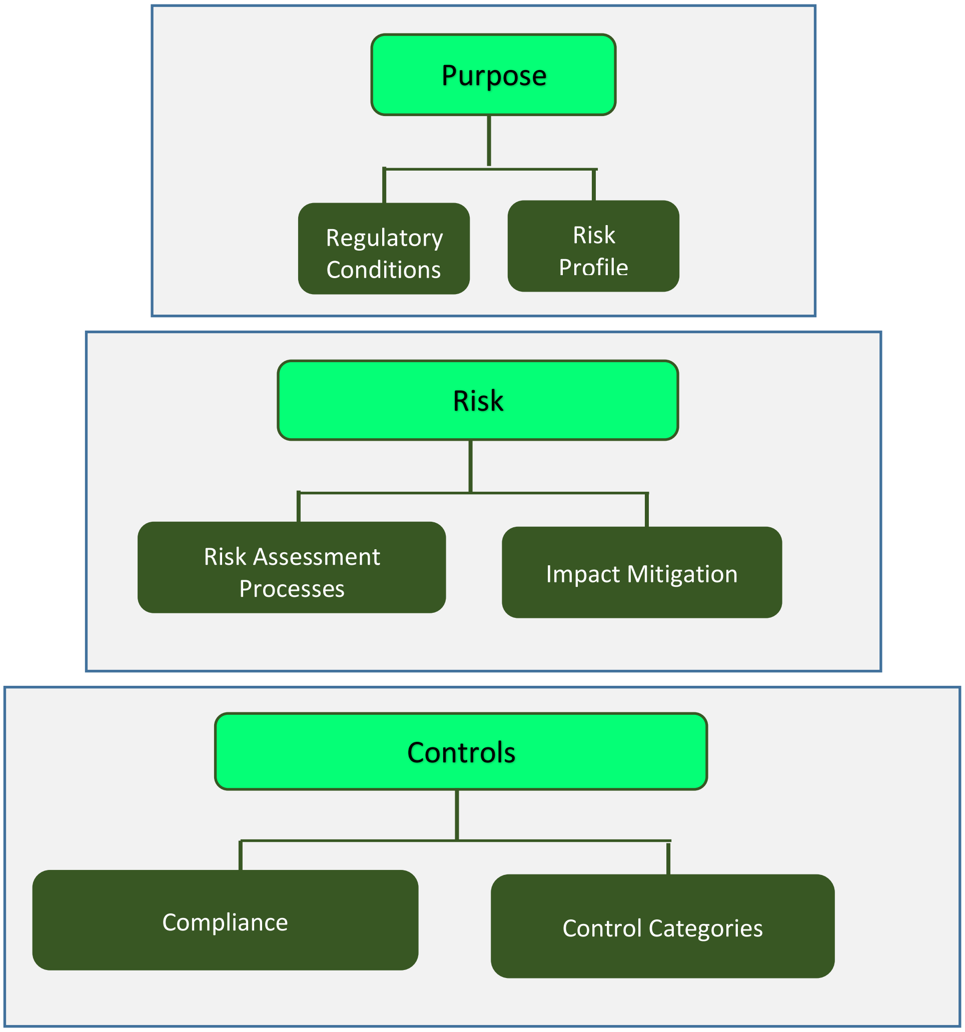


Figure 32.0: Security Reference Model

Each one of these subareas must be addressed at the system, organization and WoG levels respectively. The SecRM uses the information from the purpose and risk at each level of the government to find and classify the correct controls to secure the environment.

Purpose: The Purpose area describes the risk to business impact and regulatory environment that shapes the reasons and responsibilities for a security. Security practices must balance both risk reduction and regulatory compliance. The SecRM incorporates **regulatory compliance** at the Organization/WoG level with **risk profiles** at the system and application levels to drive security choices.

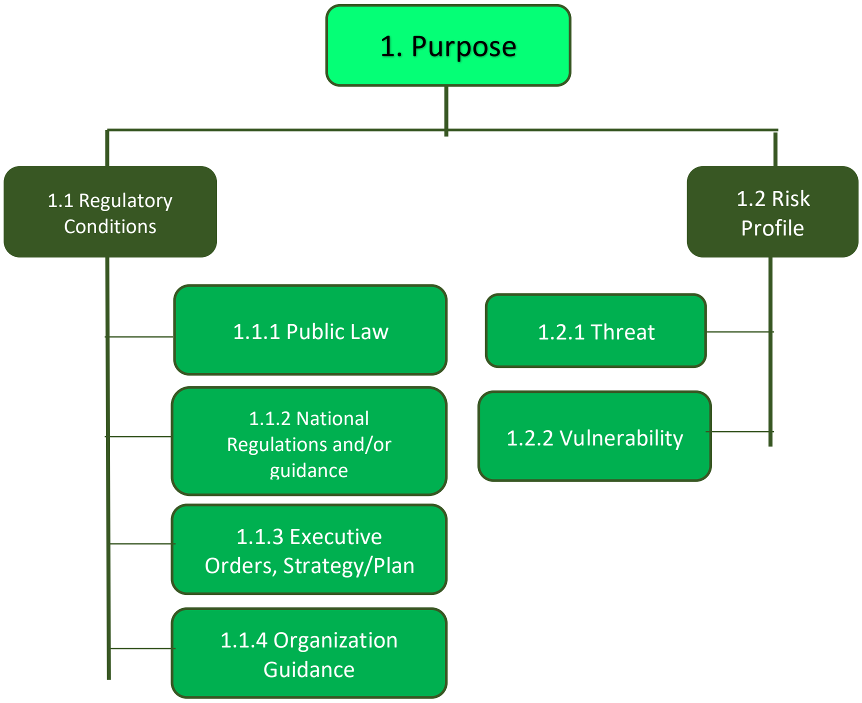

1. Purpose
1.1 Regulatory Conditions
1.2 Risk Profile
1.1.1 Public Law
1.1.2 National Regulations and/or guidance
1.1.3 Executive Orders, Strategy/Plan
1.1.4 Organization Guidance
1.2.1 Threat
1.2.2 Vulnerability

Figure 33.0: Security purpose definition

The regulatory conditions and risk profile are explained in the table A.3 in the Appendix.

Risk: Risk reduction is the ultimate reason for the application of security controls. For instance, in **NIST SP 800-30,** risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Risk is reduced through exercising control over the potential impact and/or likelihood of a vulnerability being exploited or through elimination of a threat source.

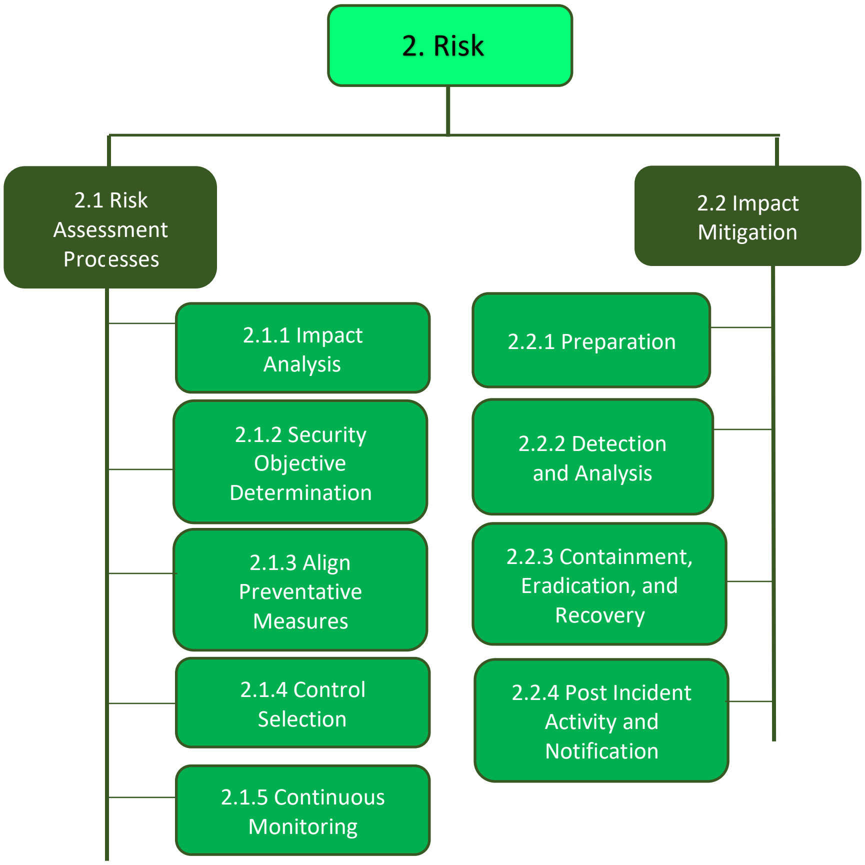

2. Risk
2.1 Risk Assessment Processes
2.2 Impact Mitigation
2.1.1 Impact Analysis
2.1.2 Security Objective Determination
2.1.3 Align Preventative Measures
2.1.4 Control Selection
2.1.5 Continuous Monitoring
2.2.1 Preparation
2.2.2 Detection and Analysis
2.2.3 Containment, Eradication, and Recovery
2.2.4 Post Incident Activity and Notification

Figure 34.0: Security risk definition

The risk assessment and impact mitigation are explained in the table A.3 in Appendix.

Controls: Ideally, the SecRM uses and refers to the overarching policies in place from the National level to classify controls for a specific public institution. The SecRM allows the architect to choose controls based on the purpose of the organization as well as by the risks faced by that particular public institution. Controls maintained or satisfied at the organization level can then be inherited at lower system or application levels. The controls also facilitates the design and/or requirements of the specific system and/or application. These controls at the national level allow public institutions and security personnel to audit or review a system.

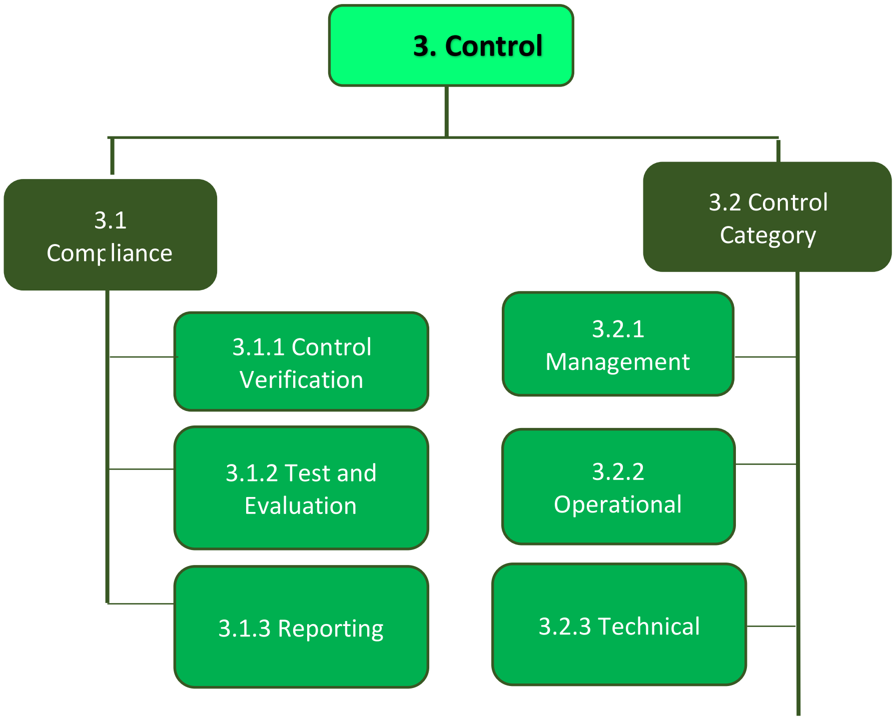


Figure 35.0: Security risk definition

The risk compliance and control category are explained in the table A.3 in Appendix.

Recommendations

Using the Security Reference Model

At both organization and WoG levels, the fundamental to using the SecRM is to adopt standards in place at the international and national security space to classify and specify implementation of security policies. These standards include ISO 27000 series, NIST SP 800 series, COBIT 5 for information security, National Information System and Network Security Standards by NITDA etc. The SecRM can then identify overlap requirements between standards and policies within organization. The policies must also be balanced with appropriate requirements so as not to preclude the organization achieving its business objectives.

The SecRM should be used:

a. To ensure that at the system or application level, controls in place at the organization level are used to facilitate the design and/or requirements of the specific system. It is critical for architects to be involved in the earliest stages of planning a system or application in order to minimize the impact sometimes involved if security is added or addressed at a later stage. It is also crucial to understand the business goals and processes that are driving decisions for a particular system or application, in addition to knowing what policies and controls will be inherited.

b. To ensure that proper security controls are placed at each level. if no control has been defined the by the implementing public institution, the system architect must put them in place. If a National law on security specifies certain action, the system level must comply whether or not the public institution capability or policy has been developed to support that law.

Best Practices

The following widely accepted best practices, guidance and standards can be adopted to implement SecRM.

1. ***ISO 2700 Series***: The ISO 27000 series was developed by the International Standards Organization. It provides a very broad information security framework that can be applied to all types and sizes of organizations. It is broken up into different sub-standards based on the content. For example, ISO 27000 consists of an overview and vocabulary, while ISO 27001 defines the requirements for the program. ISO 27002, which was evolved from the British standard BS7799, defines the operational steps necessary in an information security program. There are many more standards and best practices documented in the ISO 27000 series. ISO 27799, for example, defines information security in healthcare, which could be useful for those companies requiring HIPAA compliance. New ISO 27000 standards are in the works to offer specific advice on cloud computing, storage security and digital evidence collection. ISO 27000 is broad and can be used for any industry including government. However, like many of the ISO standards, it can be a bit daunting, and many smaller organizations are put off by the effort required to gain accreditation and the perception that it can be difficult to implement.
2. ***NIST SP 800 Series***: The U.S. National Institute of Standards and Technology (NIST) Special Publication 800 series was first published in 1990 and has grown to provide advice on just about every aspect of information security. (NIST) is at the forefront of risk guidance for the public sector. For example, the U.S. government agencies utilize NIST SP 800-53 to comply with the Federal Information Processing Standard's (FIPS) 200 requirements. It can be aligned to the ISO standards, such as ISO 9000 quality management. Because NIST contains a lot of practical guidance, it can also be adapted relatively easily to smaller and non-US organisations. In addition, the Risk Management Framework (RMF), as described in NIST SP 800-30 rev 1, provides a process that integrates information security and risk management activities into the system development life cycle. The RMF steps include system categorization, selection of security baseline controls, control implementation, control assessment, system authorization, and system monitoring.
3. ***Control Objectives for Information and Related Technology (COBIT)***: is a framework developed in the mid-90s by ISACA, an independent organization of IT governance professionals. ISACA currently offers the well-known Certified Information System Auditor (CISA) and Certified Information Security Manager (CISM) certifications. This framework started out primarily focused on reducing technical risks in organizations, but has evolved recently with COBIT 5 to also include alignment of IT with business-strategic goals. While it’s not as widely followed as others, COBIT is mostly used within the finance industry to comply with standards such as Sarbanes-Oxley.

NOTE: If public institutions want to adopt a formal risk management framework, COBIT is worth considering.

Summary: The beauty of any of these frameworks is that there is overlap between them so "crosswalks" can be built to show compliance with different regulatory standards. For example, ISO 27002 defines information security policy in section 5; COBIT defines it in the section "Plan and Organize"; Sarbanes Oxley defines it as "Internal Environment"; HIPAA defines it as "Assigned Security Responsibility"; and PCI DSS defines it as "Maintain an Information Security Policy." By using a common framework like ISO 27000, a company can then use this crosswalk process to show compliance with multiple regulations such as HIPAA, Sarbanes Oxley, PCI DSS and GLBA, to name a few.

Security controls, policy, and processes must be built into the systems development life cycle (SDLC) for information security to be implemented successfully and cost-effectively. Each organization should have a mechanism by which risk and security concerns inform the design and implementation of systems and applications, to avoid creating cost and schedule impacts due to security requirements being added at the operations and maintenance stage of the SDLC. The continuous assessment of risk and the effectiveness of controls are required throughout the entire lifecycle of the IT system.

NOTE: Implementing controls are not the primary goal of security. Rather, controls are an indispensable part of achieving the goal of reducing risk through layered security measures.

Linking security and privacy to public institution’s enterprise architecture, including performance objectives, business processes, data flows, applications and infrastructure technologies, ensures that each aspect of the business receives appropriate security and privacy considerations. Additionally, addressing security and privacy through enterprise architecture promotes interoperability and aids in the standardization and consolidation of security and privacy capabilities.

Other Recommendation: In addition with the above, public institutions must abide by Nigeria Data Protection Guideline to ensure privacy and protection of Citizens’ information.

3.2.7 Performance Reference Model (PRM)

The FEAF refers to the PRM as a framework that is designed to clearly define the cause-and-effect relationship between inputs, outputs, and outcomes and provide framework for measuring outputs and outcomes impact.

It builds from the value chain and program logic models based on line of sights concept. Line of sight is the idea that the work done at lower levels of detail has a clear path to the outcomes of the agency. The PRM Line of Sight essentially forms a value chain for tracing lower level investments and activities to higher level of outcome. This “line of sight” concept is critical for IT/ICT directors, enterprise architects, program and project management office, and key decision-makers to understand how, and to the extent, key inputs are enabling progress toward outputs and outcomes. The PRM captures this “line of sight” to reflect how value is created as inputs (such as Technology) and used to create outputs (through Processes and Activities), which in turn, impact outcomes (such as, Mission, Business and Customer Results). Guiding the entire PRM are “Strategic Outcomes,” representing broad, policy priorities driving the direction of government (Such as Security, Social welfare and Economy).

Performance is also an issue that cuts across all the reference models and levels of a public institution either as an individual organization or WoG. Therefore, PRM ensures performance is measured across all other reference models.

NGEA High-level Expectation of Performance Reference Model: The following highlights exactly what is expected of PRM. The expectations are what government policies and regulations should address while deploying IT infrastructure

Organization Strategic Outputs and Outcomes*:* A Strategic Outcome is a desired societal state or end result to which an organization's efforts are ultimately directed. The strategic outputs are immediate deliverables of any project/program. In order to measure performance , each public institution is expected to set its strategic outputs and outcomes which are in line with its functions and mandates. The strategic outputs and outcomes in line with the mandates/functions form the basis upon which the organization will be measured. In order to measure public institutions' IT performance, they should be and are going to be measured against their expected strategic outputs and outcomes enabled or to be enabled by IT adoption as inputs.

Aligning with NGEA Vision, Principles, Value Propositions, WoG Operating Model and Reference Models: It is expected that each public institution aligns with what NGEA has set as vision, principles, value propositions, coordinating operating model and reference models. Adhering and meeting every requirement in NGEA principles, value Propositions, WoG operating model and reference models will enable and propel achievement of NGEA vision. Every public institutions will be measured against these requirements for their IT projects/programs.

The PRM Abstract Model

The PRM abstract model is structured around four areas: Measurement Areas, Measurement Categories, Measurement Groupings, and Measurement Indicators.

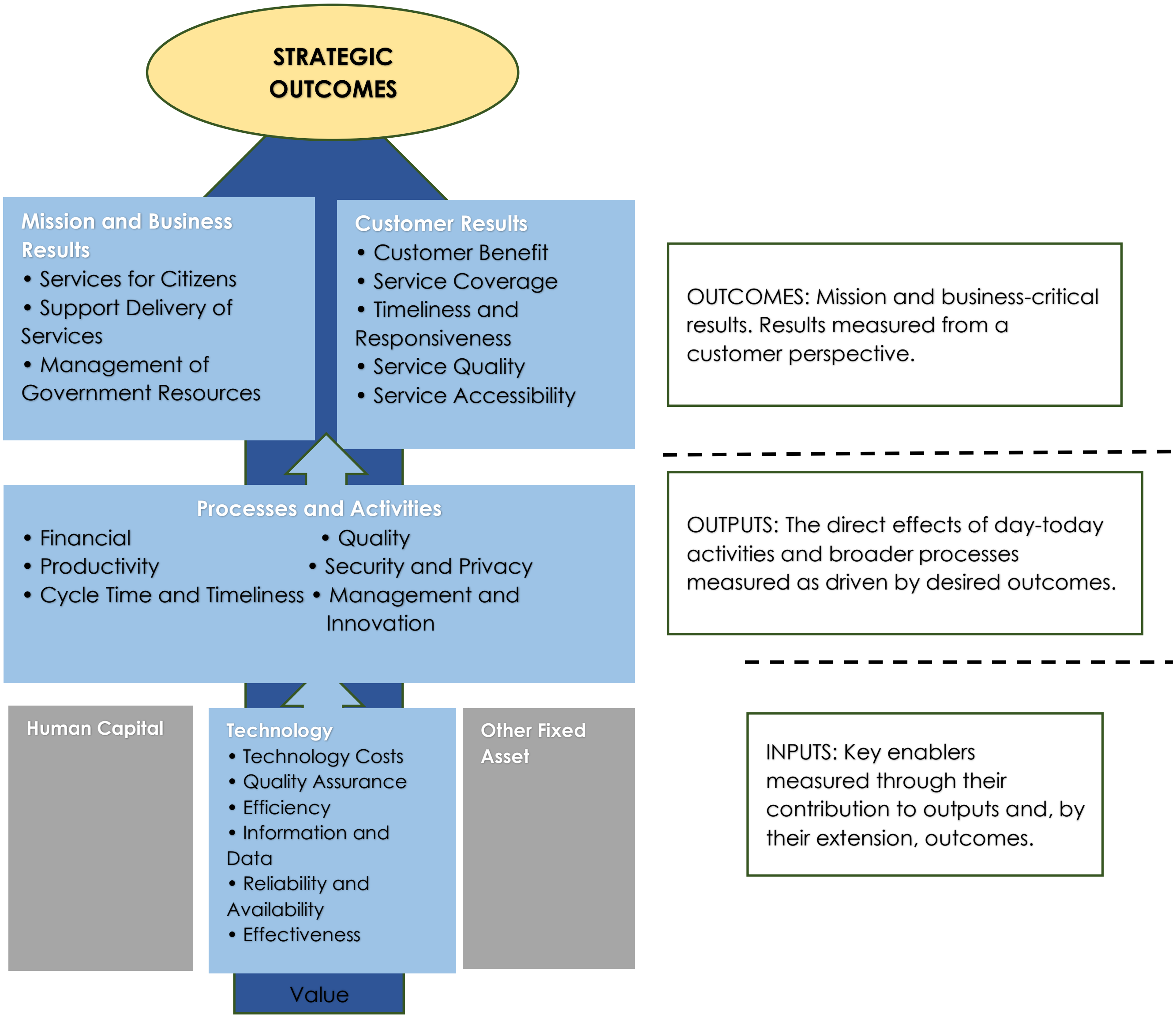

STRATEGIC OUTCOMES
Mission and Business Results
• Services for Citizens
• Support Delivery of Services
• Management of Government Resources
Customer Results
• Customer Benefit
• Service Coverage
• Timeliness and Responsiveness
• Service Quality
• Service Accessibility
OUTCOMES: Mission and business-critical results. Results measured from a customer perspective.
Processes and Activities
• Financial
• Productivity
• Cycle Time and Timeliness
• Quality
• Security and Privacy
• Management and Innovation
OUTPUTS: The direct effects of day-today activities and broader processes measured as driven by desired outcomes.
Human Capital
Technology
• Technology Costs
• Quality Assurance
• Efficiency
• Information and Data
• Reliability and Availability
• Effectiveness
Other Fixed Asset
Value
INPUTS: Key enablers measured through their contribution to outputs and, by their extension, outcomes.

Figure 36.0: PRM reference model.

Measurement Areas: Refer to the high-level organizing framework of the PRM capturing aspects of performance at the output levels. This layer is directly linked to the performance objectives established at the public institution and program/project levels. The PRM specifies six measurement areas: Mission and Business Results, Customer Results, Processes and Activities, Human Capital, Technology, and Other Fixed Assets.

Mission and Business Results: Captures the outputs organizations seek to achieve that are usually developed during the agency budget and strategic planning process. To ensure the organizations' identified outputs are appropriately aligned to what they actually do, the Mission and Business Results Measurement Area is driven by the Business Reference Model (BRM). More specifically, the PRM's Measurement Categories are the same as the BRM's Business Areas (e.g. Sector) and Lines of Business (e.g. specific functions/mandates of a public institution). The Measurement Groupings of the PRM are the same as the Sub-functions (e.g. departments/subsidiaries to carry out certain part of function/mandate) of the BRM. These areas of the BRM seek to identify the purpose of the government activity.

By extension, the Mission and Business Results Measurement Area of the PRM identifies the extent to which those purposes are being achieved. It is comprised of the following Measurement Categories:

1. Services for Customers;
2. Support Delivery of Services; and
3. Management of Government Resources

For instance, to identify the Mission and Business Results associated with an IT initiative, a public institution needs to refer to its performance objectives.

Customer Results Measurement Area: Captures how well an agency or specific process within an agency is serving its customers—and ultimately citizens. The Customer Results Measurement Indicator captured in this Measurement Area will be associated with the most external customer of the process or activity the IT initiative supports.

The purpose of the Customer Results Measurement Area is to identify the customer relationship and articulate how it can be measured over time. The Customer Results Measurement Area is comprised of the following Measurement Categories:

1. ***Customer Benefit***: Customer satisfaction levels and tangible impacts to customers as a result of the products or services provided
2. ***Service Coverage***: The extent to which the desired customer population is being served and customers are using products and services
3. ***Timeliness and Responsiveness***: Time to respond to customer inquiries and requests and time to deliver products or services
4. ***Service Quality:*** Quality from the customer's perspective and accuracy of responses to customer inquiries
5. ***Service Accessibility***: Availability of products and services to customers and the extent of self-service options and automation

Processes and Activities Measurement Area: Captures the outputs directly resulting from the process an IT initiative supports. This Measurement Area also captures key aspects of processes or activities required to be monitored and/or improved. The desired output for a process or activity should strongly influence:

1. Whether technology is needed to improve or support the process, and
2. If so, what technology is needed to help the processes or activities achieve the desired outputs.

Processes and Activities Measurement Area begins with the BRM. The BRM includes a Mode of Delivery Business Area designed to identify, at a very high level, the process being used to achieve an intended purpose. The Measurement Indicator(s) selected should be an extension of the Mode of Delivery aligned with the IT initiative. For example, if an IT initiative aligns with the Security agenda in the business areas and lines of business in the BRM, the PRM can be used to determine the quality of how that security service is delivered.

The Processes and Activity Measurement Area is comprised of the following Measurement Categories:

1. ***Financial:*** Achieving financial measures, direct and indirect total and per unit costs of producing products and services, and costs saved or avoided;
2. ***Productivity*****:** The amount of work accomplished per relevant units of time and resources applied;
3. ***Cycle Time and Timeliness*****:** The time required to produce products or services;
4. **Quality**: Error rates and complaints related to products or services;
5. ***Security and Privacy***: The extent to which security is improved and privacy addressed having considered the security and privacy laws, policies and regulations of the country and other operating environments (e.g. foreign countries);
6. ***Management and Innovation:*** Management policies and procedures, compliance with applicable requirements, capabilities in risk mitigation, knowledge management, and continuous improvement.

Processes and Activities Measurement Area**:** Captures key elements of performance directly relating to the IT initiative. An IT initiative can include applications, infrastructure, or services provided in support of a process or program. In particular, this measurement is related to ARM, IRM and in some cases SecRM.

While these IT-specific aspects of performance (e.g. percent system availability) are important, they alone do not truly assess the value of an IT initiative to overall performance. The Technology Measurement Area attains far more relevance only when used with other Measurement Areas to get a full and accurate picture of overall performance.

The Technology Measurement Categories and Groupings do not represent exhaustive lists. Public institutions may, and should, have additional Technology measures used as part of their **IT Capital Planning and Investment Control (CPIC)** and **Systems Development Lifecycle processes.** The Technology Measurement Area is comprised of the following Measurement Categories:

1. ***Technology Costs:*** Technology-related costs and costs avoided through reducing or eliminating IT redundancies
2. ***Quality Assurance***: The extent to which technology satisfies functionality or capability requirements or best practices, and complies with standards
3. ***Efficiency*****:** System or application performance in terms of response time, interoperability, user accessibility, and improvement in technical capabilities or characteristics
4. ***Information and Data:*** Data or information sharing, standardization, reliability and quality, and storage capacity
5. ***Reliability and Availability***: System or application capacity, availability to users, and system or application failures

6. ***Effectiveness:*** Extent to which users are satisfied with the relevant application or system, whether it meets user requirements, and its impact on the performance of the process(es) it enables and the customer or mission results to which it contributes.

Human Capital Measurement Area**:** Currently, PRM does not include specific Measurement Categories for Human Capital. Public institutions are advised to adhere to Public Service Rules and other rules and regulations specific to a particular Business Areas and Lines of Business.

Other Fixed Assets Measurement Area**:** Also, PRM does not include specific Measurement Categories for other fixed assets. Public institutions are advised to adhere their specific rules and regulations.

Measurement Categories: Refer to collections within each measurement area describing the attribute or characteristic to be measured. For example, the Customer results Measurement Area include five Measurement Categories: Customer Benefit, Service Coverage, Timeliness and Responsiveness, Service Quality and Service Accessibility.

Measurement Groupings: Refer to further refinement of categories into specific types of measurement indicators. For the Mission and Business Results Measurement Area, these groupings align to the Sub-functions of the BRM.

Measurement Indicators*:* Refer to specific measures, e.g., number and/or percentage of customers satisfied, tailored for a specific BRM Line of Business or Sub-function, program/project or IT initiative.

Each public institution's strategic road map and planning process establishes specific programs and objectives to meet the needs of its stakeholders and customers. These programs are implemented to deliver citizen services enabling public institutions to achieve desired performance objectives. Performance management, which is critical to the successful use of the PRM and the EA, ensures an organization's IT investments can be directly linked to its performance objectives.

Recommendations

Using the Performance Reference Model

Performance Measurement Template**:** Each of the measurement areas can be measured using measurement categories, groupings and indicators.

The table 6.0 is a template for measuring each business area. This creates the actual inventory of measurement indicators.

Table 6.0: Performance measurement template

Measurement Category	Measurement Grouping	Measurement Indicators

For instance, the table 6.0 captures performance measurement for technology measurement areas. This captures key elements of performance that are directly related to the IT initiative. An IT initiative generally can include applications, infrastructure, or services provided in support of a process or program.

Table 7.0 Performance measurement example

Measurement Category	**Measurement Grouping**	**Measurement Indicators**
Technology Costs: Technology-related costs and costs avoided through reducing or eliminating IT redundancies.	Overall Costs	
	Licensing Costs	
	Support Costs	
	Operations and Maintenance Costs	
	Training and User Costs	
Quality Assurance: The extent to which technology satisfies functionality or capability requirements or best practices, and complies with standards.	Functionality	
	IT Composition	
	Standards Compliance and Deviations	
Efficiency: System or application performance in terms of response time, interoperability, user accessibility, and improvement in technical capabilities or characteristics.	System Response Time	
	Interoperability	
	Accessibility	
	Load Levels	
Information and Data - Data or information sharing, standardization, reliability and quality, and storage capacity.	External Data Sharing	
	Data Standardization or Tagging	
	Internal Data Sharing	
	Data Reliability and Quality	
	Data Storage	
Reliability and Availability - System or application capacity,	Availability	

availability to users, and system or application failures.	Reliability	
Effectiveness: Extent to which users are satisfied with the relevant application or system, whether it meets user requirements, and its impact on the performance of the process(es) it enables and the customer or mission results to which it contributes.	User Satisfaction	
	User Requirements	
	IT Contribution to Process, Customer, or Mission	

Therefore, each public institution is required to develop its performance measurement template

As public institutions use the PRM for their specific IT initiatives, they will create the inventory of measurement indicators.

Performance Reporting

1. ***Describe the relationship between investment and organization strategic goals.*** A narrative explanation of the investment's specific contribution to mission delivery and management support functions is required to help each public institution measure how the investment contributes to the agency target architecture and links to performance objectives in the published agency strategic plan.
2. ***Provide investment-specific performance measures that quantify the intended performance benefits.*** Each measure must be categorized using performance measurement template, and investment owners must ensure that the measures are balanced and drawn from multiple measurement categories. Every government agencies are required to develop IT dashboard to performance metric.
3. Report on investment results using these measures annually.

3.4 NGEA IT Engagement Model (NITEM)

Every IT project must not only meet its short-term goals of the owner (public institution) but also help implement the WoG architecture. Ensuring that every IT project that is being added to the enterprise (Federal Government-wide) helps and contributes to building an efficient WoG architecture requires the engagement of key stakeholders in the design, implementation and the use of IT to enable business process capabilities that in turn create better and improved digital services. IT engagement model is a system of governance mechanisms assuring that business and IT projects achieve both local (public institution) and WoG (One Government) objectives.

Therefore, the NITEM is a governance mechanism that is actually responsible for accomplishing the NGEA vision, ensuring the chosen operating model (coordination operating model) for the WoG or One Government Agenda is adhered to, making sure public institutions are successfully migrated from lowest EA maturity (silo) stage to the highest (Service modularity architecture) stage and ensuring specifications and recommendations in the EA reference models are implemented accordingly. The NITEM coordinates these activities while ensuring (for now) there is strong alignment of FPIs' IT investment and their business objectives. This is to ensure expected values are generated from IT investments.

The IT engagement model for an enterprise management has different stakeholders each of which exists on both **Business and IT** sides of the enterprise. The different perspectives, objectives and interests of these two groups across within and across government organizations create two challenges: Coordination and Alignment. Accordingly, the key considerations for using the NITEM is to address the two issues:

1. ***Coordination:*** Coordination of IT activities between the interest of the WoG and individual government organization as well as how IT is being managed at both levels.
2. ***Alignment:*** Alignment of the interests and efforts of two major stakeholders (Business and IT) at the WoG and organizational levels. The business and IT sides of the WoG and public institutions have different perspectives and interests

The ability to effectively coordinate IT activities within and across government organizations and the alignment of business and IT at both levels greatly determine the success of the NGEA.

The research in enterprise architecture as a strategy at MIT Sloan School's Center for Information System Research (CISR) describes three components of IT engagement model. The three components are: IT Governance, IT Coordinating Mechanism and IT Project Management.

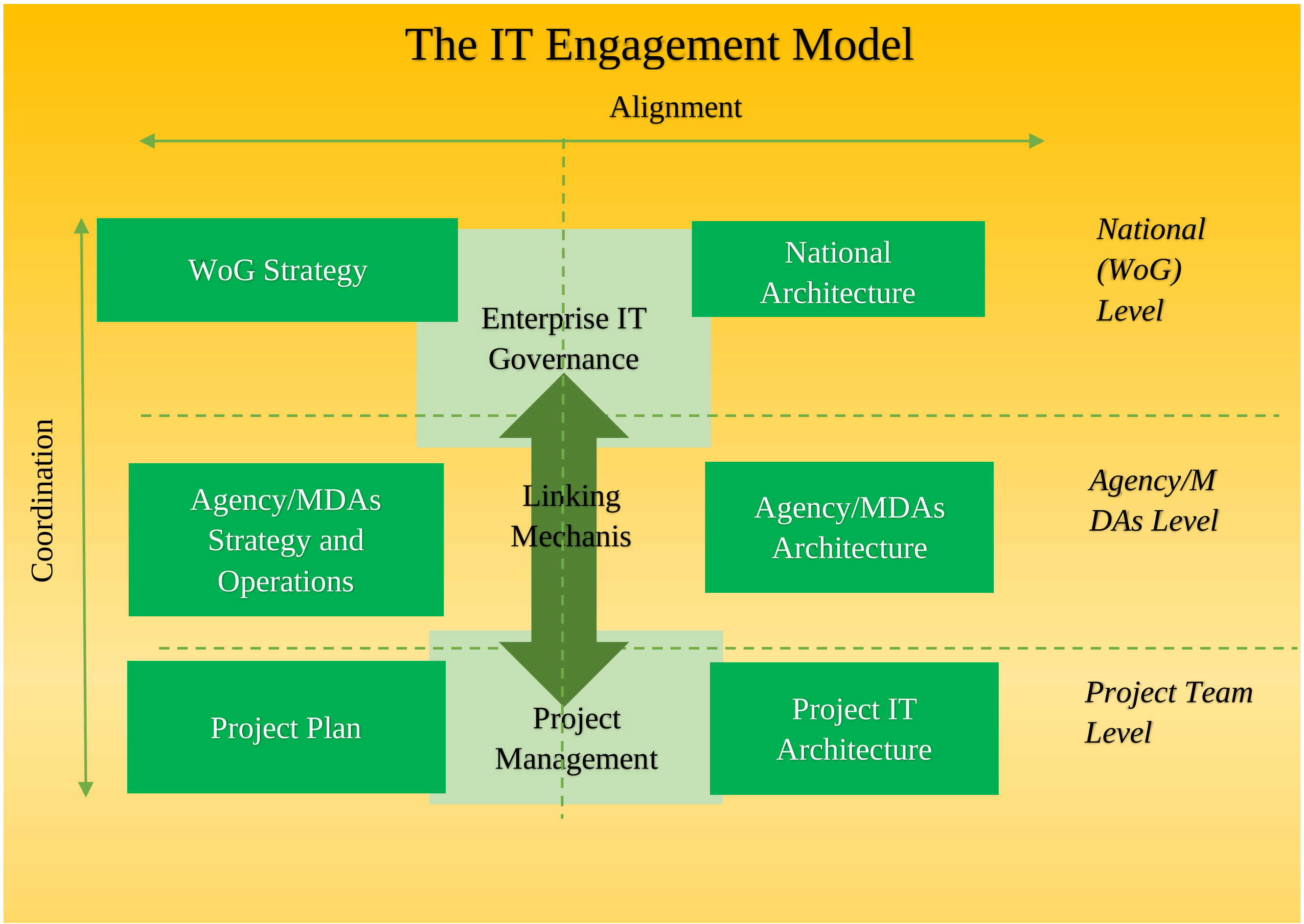


Figure 37.0: The IT engagement model

These concepts are explained as follows:

3.4.1 Organization/government-wide (WoG) IT governance

IT governance covers decision rights and accountability frameworks to encourage desirable behaviors in the use of IT. It is the most important factor in generating business/governance value from IT investments and adoption. In this context, IT governance provides structure for those who set strategic directions, make IT investment and adoption decisions and those who should be accountable for IT projects implementation at each public institution or for the WoG. It focuses on the management and use of IT to achieve organization/ WoG performance goals. IT governance encompasses five major decision areas related to the management and use of IT in government organizations all of which should be driven by the coordination operating model. They are:

1. ***IT principles:*** High-level statements/decisions about how IT is used to achieve the public institution's mandates/functions or the strategic goals of IT in organization's business. These principles should be exploited in accordance with the NGEA principles and the public institution's mandates/functions as addressed in the Business Reference Model for adopting IT in running government's businesses.
2. ***Enterprise Architecture:*** The organizational logic for business processes and IT infrastructure reflecting the integration and standardization requirements of the WoG operating model (i.e. Coordination Operating Model). Key to getting this done is to focus on identifying the requirements for customers' interfaces, processes, data, technologies and applications that take the coordinating operating model from vision to reality. This will be achieved by following all the expectations, specifications and best practices requirements in the NGEA reference models.
3. ***IT Infrastructure:*** Coordinated and shared IT services that act as foundation upon which business applications and digital services are built to ensure efficient IT environment. A better IT infrastructure will be achieved by following the specifications, best practices and recommendations in the Infrastructure Reference Model and standardized technology architecture stage of the enterprise architecture maturity model.
4. ***Business application needs:*** Business requirements for purchased or internally developed IT applications for each public institution or core/common IT applications for WoG. The key to making informed and suitable decisions for business application needs is to follow the expectations, specifications and recommendations in the business, service and data reference models.
5. ***Prioritization and Investment:*** Decisions about how much and where to invest in IT, including project approval and justification techniques by each public institution and the WoG. Effective IT prioritization and investment is a function of adhering to expectations, specifications and recommendations in the performance reference model.

NOTE: The first step in designing IT governance is to determine who should make, and be held accountable for, each of these decision areas.

Recommendation: The CEO, top management and ICT Director/Head of ICT in each organization shall be responsible for the choice made in the five IT Governance decision areas.

Table 8.0: Decision areas

Key issues for IT decision	
IT principles	• How does the operating model translate IT principles to guide IT decision making? • What is the role of IT in the operation model? • What are the IT- desirable behaviors? • How will IT be funded – by the Federal Government or by Public Institutions?

Enterprise Architecture	• What are the public institutions' core business processes? How are they related? • What information drives these core processes? How must this information be integrated? • What technical capabilities should be standardized government-wide to support IT efficiencies and facilitate process standardization and integration? • What activities must be standardized government-wide to support data integration? • What technology choice will guide the company's approach to IT initiatives?
IT infrastructure	• What infrastructure services are most critical to achieving the company's operating model? • What infrastructure services should be implemented government-wide? • What are the service-level requirements of those services? • How should infrastructure services be priced? • What is the plan for keeping underlying technologies up to date? • What infrastructure service should be outsourced
Business Application Needs	• What are the service and business process opportunities for new business applications? • How can government's business needs be addressed within architectural standards? • When does a business need justify an exception to the standards? • Who will own the outcomes of each project and institute organizational changes to ensure value? • What strategic experiments should be taken on? How should success be measured?
IT Investment And Prioritization	• What process changes or enhancements are strategically most important to the public institutions? • What is the distribution in the current IT portfolio? Is this portfolio consistent with the WoG's objectives? • Do actual investment practice of public institutions reflects their relative importance? • What is the right balance between top-down and bottom-up projects to balance standardization and innovation?

As each project is being added to the enterprise (Federal Government-wide), IT engagement model influences and monitors project decisions so that individual solutions are guided by enterprise architecture specifications as decisions are made at different levels: WoG (National), Organization (FPIs) and functional (organization's departments/business functions).

3.4.2 IT Project Management

After decisions have been made in those five areas, the next step is to adopt and apply a standardized methodology to the identified IT projects. The major objectives of such standard method are its competitive capabilities to ensure better **cost** effectiveness, improved **quality** and **timeliness** of project delivery. The chosen project management methodology should have well-defined process steps with clear deliverables to be reviewed at regular checkpoints.

IT projects have long been guided by a project life cycle. There are variation of life cycle that define a set of Four (4) to Eight (8) project phases each with a specific set of objectives, deliverables and metrics. A good project management establishes a set of "checkpoints" that check on projects' progress and assess their chances for meeting their goals. At each checkpoint, the IT project should go through a number of business and IT reviews.

An IT project is managed by the public institution's ICT department/unit or equivalent in collaboration with Project Management Office/Department/Unit. To ensure government-wide coherence in managing and implementing IT projects, there is a need for a common/single approach to IT project management. Standardized stages should be followed regardless of the project management processes or methodology adopted.

The following five stages are proposed as uniform and consistent stages government-wide for managing IT projects. An IT project will go through these stages regardless whether you are running a traditional waterfall, hybrid (a combination of agile and waterfall) or an agile project, the difference is you may have multiple iterations of stages with agile approaches.

1. ***Stage 1- Proposal:*** The first stage involves development of proposal for the IT project. The proposal covers IT project description & problem statements, purpose/goal & specific objectives, project justification & business cases, project scope and deliverables, timelines & milestones, assumptions and risk factors, budget cost & resources, key performance indicators (KPIs) and expected outcomes. In addition, the stage 1 also seeks for the approval of the organization's Management to embark on the project.

2. ***Stage 2-Requirements Analysis*****:** The approval of the proposal by Management should lead to stage 2 where the project requirement analysis is carried out. The requirement analysis should consist of the following: feasibility study, definition of functional and non-functional requirements, project design and architecture based on organization's specific Enterprise Architecture and also in line with NGEA requirements, project specifications and decision on appropriate and suitable technologies.

NOTE: If the project is not an IT system development, this stage might be skipped. However, in both cases approvals of the project by Management, Bureau of Public Procurement (BPP), IT Project Clearance Body (NITDA) and the Federal Executive Council are required depending on the regulatory requirements by each of these bodies.

3. ***Stage 3-Implementation***: The implementation stage involves procurement, solution development and/or programs execution, change management within organization and government-wide. The change management should entail capacity building for the system users in addition to other standard components of change management. This stage also involves integration of the solution with existing IT systems within the organization and with external systems of the cooperating government organizations where integrated or cross-portfolio digital service delivery is required. The last step at this stage is testing to ensure solutions meet the functional and non-functional requirements, design and architectural requirements etc.

4. ***Stage 4-Go live:*** The stage 4 involves release of the solution into production environment after the system has been tested successfully. It also involves support, performance measurement in live environment and maintenance.

5. ***Stage 5- Project Closing*****:** The last stage handovers the project to the project owners for outright maintenance. Project closing should not be the end of the project, the project should be monitored and evaluate in the long run to determine the effectiveness or otherwise of the solution. IT project monitoring and evaluation is a performance issue that can be managed at the performance reference model.

3.4.3.Coordinating/Linking Mechanisms

It has been proved that enterprise with effective IT governance and disciplined project management can still have ineffective IT engagement. The coordinating/Linking mechanisms connect organization and government-wide IT governance and projects. Good IT governance ensures that there is clear direction on how each public institution builds its IT capabilities to be leveraged and accomplished business and WoG objectives. Good IT project management ensures that projects are implemented effectively, efficiently and in a consistent manner to maximize learning while good coordinating/linking mechanisms ensure that as each IT project is being added to the enterprise (individual public organizations and the collective WoG), it incrementally builds and adds to the foundation and that the design of the foundation (the coordinating operating model and enterprise architecture) is informed by the projects.

There are three important types of linking mechanisms for any IT engagement model: **architecture linkage** (linkage of requirements for data, processes, applications, IT infrastructure and the people needed to deliver business functions and strategic goals), **business linkage** (mandates/functions) and **alignment linkage** (Business-IT).

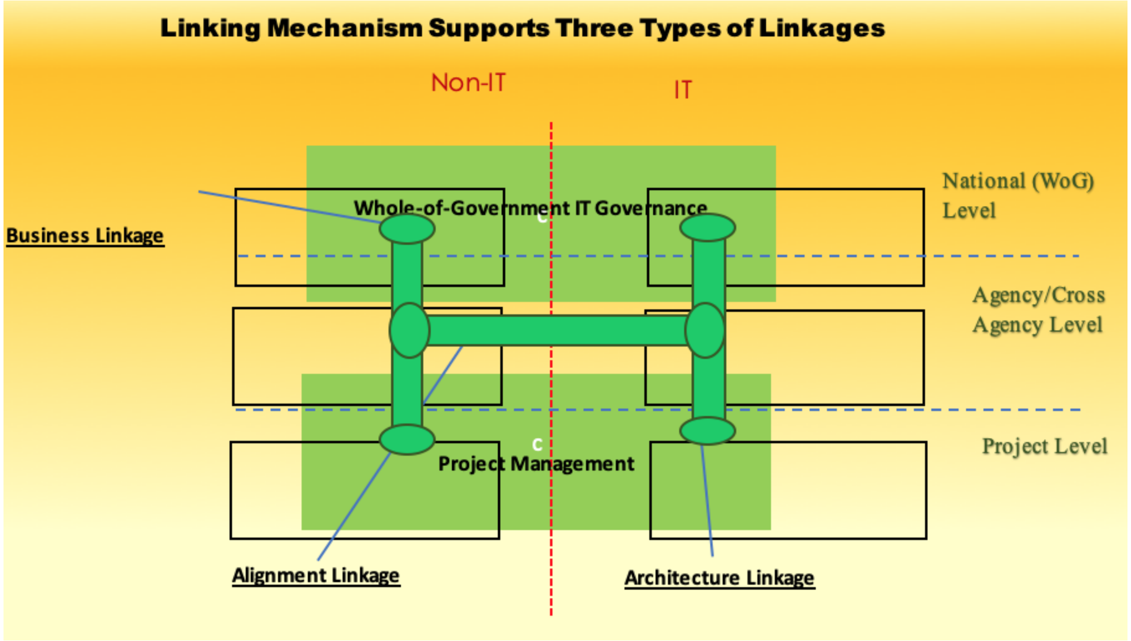


Figure 38.0: Linking Mechanisms

Architecture linkage: The architecture linkage establishes and updates standards, reviews projects for **compliance** (Coordination operating model and architecture reference models) and approves **exceptions** (architecture exception processes). It connects the IT governance decisions about architecture with project design decisions.

At the public institution level, the Enterprise Architecture unit/Enterprise Architecture Team will be responsible for architecture linkage. Where this does not exist, the Management and the Director/Head of ICT will be responsible for architecture linkage government-wide.

Business Linkage: The business linkage ensures that business goals are translated effectively into project goals. Business linkage coordinates IT projects, focuses IT projects on addressing specific problems in the best possible way and connects them to larger WoG and government transformation agenda. Business linkage also include incentive programs for system users (change management, training etc.) to guide the right behavior as new projects demand new ways of doing things. The Management and the Directors/Heads of ICT of government organizations are responsible for business linkage tasks.

Alignment Linkage: The alignment linkage mechanisms ensure ongoing communication and negotiation between IT and business concerns. The Directors/Heads of ICT as a member of Management of government organizations are responsible for translating and aligning back and forth between business goals and IT constraints. Other mechanism for achieving alignment linkage is project management Office/Department/Unit of an organization and the National IT Project Clearance Body (NITDA)

Based on the linking mechanism requirements, the following mechanisms in table 8.0 are required to be instituted within government organizations and government-wide to ensure implementation of the linking mechanisms.

Table 9.0: The proposed mechanisms for Linking Mechanisms

Mechanism	Availability Government-wide	Responsibility
ICT Department (Director/Head ICT)	Not available in all public	Linking Mechanisms (Architecture, Business and Alignment linkages)
Project management Office/Department/Unit	Not available in all public institutions	Alignment linkage
Enterprise Architecture unit/Architecture Review Committee	Not available in all public institutions	Architecture linkage
National IT projects Clearance Committee	Available: Covers for all Federal Government organizations	Linking Mechanisms (Architecture, Business and Alignment linkages)

On the overall, the IT engagement model will be achieved through the following established mechanisms.

Table 10.0: Mechanisms for achieving IT engagement model.

LEVEL	MECHANISM	ACTION BY/RESPONSIBILITY AND MECHANISM OPTIONS	
		Responsibility	**Mechanism Options**
Organization	CEOs; Management, Directors/Heads, ICT; Project Management Office/Department/Unit; Enterprise Architecture unit/Architecture Review Committee	CEOs	IT Governance and Business linkage (in Linking mechanisms)
		Management	IT Governance and Business linkage (in Linking mechanisms)
		Directors/Heads, ICT	IT Governance, Project management and linking mechanisms
		Project Management Office/Department/Unit	IT Project management and alignment mechanism (in Linking mechanisms)

		Enterprise Architecture unit/Architecture Review Committee	Architecture linkage
Government-wide (WoG)	**National IT Project Clearance Body** (by NITDA); and **Federal Executive Council** (FEC)	**National IT Project Clearance Body:** (Linking mechanisms)	Architecture, Business and Alignment linkages
		FEC	Approves IT projects based on recommendations by **National IT Project Clearance Body** (NITDA) through and Bureau of Public Procurement (BPP)

NOTE: ***The linking mechanisms act as watch dog to ensure IT projects are implemented according to the specifications and requirements of the IT governance, IT project management, NGEA principles, Coordination operating model and architecture reference models.***

The IT Project Clearance Body (NITDA) is absolutely responsible for carrying out the linking mechanism responsibilities/tasks at the WoG level.

SECTION FOUR: NGEA Implementation and Compliance

All Public Institutions at the Federal levels, ICT Product/Service Providers for public institutions, professional bodies who practice in the field of IT, development partners that support Nigeria in IT projects implementation are to comply with the provision of the NGEA.

Specially, the following are responsible for compliance with the provision of NGEA in addition to the responsibilities and mechanisms mentioned in table 7.0 and 8.0 in the IT engagement model section.

1. ***FPIs' CEOs***: are responsible for the approval of IT projects on behalf of their organizations. Hence, each CEO is totally responsible for setting strategic direction across the organization for the implementation NGEA vision, principles, operating model, reference models, IT engagement model and the governance structure.
2. ***FPIs' Directors/Heads of ICT***: are responsible for the translating every provision of the NGEA to the CEOs, the Management and the entire organization. They act as the Chief Information Officers for their respective organizations and in that also responsible to ensure the organizations business and IT alignment. They are to carry their organization along while implementing NGEA vision, principles, operating model, reference models and IT engagement model.

   Thus, they are required to critically study, understand the NGEA and ensure that their respective organizations comply with these provisions. This will ensure their IT projects follow all the recommendations, specifications and requirements in the NGEA while submitting them for IT projects clearance.

   NOTE: The CEOs, the Management and the Directors/Heads of ICT are jointly responsible for approving architecture exceptions that are recommended by ICT department or EA unit at the organization level.

3. ***Federal Government IT Projects Approving and Clearance Bodies:*** Specifically, the IT project clearance body of NITDA is responsible for ensuring that every IT project submitted for clearance adheres to all the provision of the NGEA. They are also responsible for **approving architecture exceptions and waivers**.

   While NITDA performs these responsibility, all government procurement departments/units and Bureau of Public Procurement (IT procurement), Project management offices/Department/units and Federal Executive Council etc., as gate keepers to government IT projects, are similarly responsible for ensuring compliance with the provisions of NGEA.

   Where it is discovered by these approving bodies that an IT project flouts the provisions of the NGEA, such approval should be withheld/denied and the applicant should be advised to comply.

NOTE: While clearing IT projects , it is the duty of the IT project approving and clearance body to identify any deviation from NGEA architecture requirements and call the attention of the concerned party for a correction. Exceptions and waivers shall be allowed strictly on National Security reasons and/or special enabling laws/regulations that have to do with the functions/mandates of the concerned public institution.

Notwithstanding the above compliance entities, the following shall also assist with ensuring compliance with the NGEA:

1. ***Development Partners****:* Development partners who provide financial, technologies and human resources assistance to the country by implementing IT projects shall comply with provisions of the NGEA.
2. ***IT Consultant and All ICT Providers:*** They bid, supply and implement IT projects for the Federal Government. Therefore, they are also responsible for complying with the provisions NGEA while implementing government IT projects.

4.1 NGEA Implementation Governance Structure

Aside the regular compliance enforcement by IT Project Clearance bodies of NITDA on every IT project submitted for approval, a complementary governance structure will be set up to promote and ensure full implementation of NGEA at all levels.

A National strategic governance structure called "**NGEA Governing Committee**" shall be set up by NITDA to ensure promotion and implementation of NGEA.

4.2 NGEA Governing Committee

1. NGEA shall adopt the same governing committee established for the **Nigerian Government Interoperability Framework (Ne-GIF)**.
2. The NGEA Governing Committee shall consist of the following:
   a. A Coordinator
   b. The Head of IT or e-Government Department/Unit from each of the following organizations:
      I. Federal Ministry of Communication
      II. National Information Technology Development Agency
      III. Office of the Secretary General of the Federation
      IV. Federal Ministry Finance
      V. Nigeria Communications Commission
      VI. National Identity Management Commission
      VII. National Population Commission
      VIII. Nigerian Immigration Services

IX. Central Bank of Nigeria
X. Federal Mortgage Bank
XI. Nigeria Social Insurance Trust Fund
XII. National Bureau of Statistics
XIII. Independent National Electoral Commission
XIV. Federal Inland Revenue Services
XV. Joint Tax Board
XVI. Corporate Affairs Commission
XVII. National Health Insurance Scheme
XVIII. Office of the Security Adviser
XIX. Federal Road Safety Corps
XX. Pension Commission
XXI. Nigerian Police Force
XXII. Nigerian Prison Service
XXIII. Galaxy Backbone
XXIV. Budget office of the Federation
XXV. National Lottery Regulatory Commission
XXVI. Nigeria Communication Satellite
XXVII. Bureau of Public Procurement
XXVIII. Presidential Enabling Business Environment Council (PEBEC)
XXIX. Chairman, Committee of ICT Directors of Tertiary Institutions

c. However, where an organization has the Head of IT department/unit and Head of e-Government Department/unit, both shall be a member of the NGEA Governing Committee.

d. One IT professional in the Governing board from each of the following Professional Bodies:
I. Computer Professional (Registration Council) of Nigeria (CPN)
II. Nigeria Computer Society (NCS)

e. One IT professional in the Management Cadre from each of the following:
I. Nigeria Inter-Bank Settlement System (NIBSS)
II. Organized Private Sector

3. Considering NITDA's IT regulatory mandate, NITDA (through a representative from its e-Government Development and Regulation Department) shall be the Coordinator of the Committee.
4. A third of the members of NGEA Governing Committee and the Coordinator or his/her representatives shall constitute a quorum.
5. The Committee shall amongst other related things:

a. Monitor stakeholders' compliance with the provisions of the framework;
b. Meet annually to assess the compliance level of stakeholders with the provision of the framework;

c. Coordinate (where necessary) or assist in the development, promotion and adoption of models, standards, tools, guidelines and policies that will help ensure the actualization of NGEA; and

d. Coordinate the review and update of the framework in line with the provision the NGEA

4.4 EA Unit

1. All FPIs are encouraged to set up EA Division or Unit as part of IT/ICT/e-Government department. The EA division or unit shall be responsible for:

    a. Communicating the NGEA vision, principles, requirements for coordination operating model and reference models and other specifications to ensure a better understanding and coherent implementation of NGEA in the organization;

    b. Helping the organization develop its Enterprise Architecture in line with the provisions of the NGEA;

    c. Aligning the NGEA with the organization's EA, ensuring compliance with the provisions of the NGEA and recommend architecture exceptions/waivers for approval to ensure coherence implementation within organization and government-wide

    d. Linking and aligning the organization's ICT policy/strategy with its mandates/functions through the Enterprise Architecture;

    e. Facilitating compliance to other National ICT standards, Guidelines and Frameworks (e.g. Nigerian Interoperability Framework, Standards and Guidelines for Government Websites) by NITDA and other ICT statutory bodies;

NOTE: Where EA unit does not exist, the IT/ICT or e-Government department shall fully assume the responsibility of the EA unit. Where EA unit exists, IT/ICT or e-Government department directs the activities of the EA unit and EA unit reports to IT/ICT or e department.

4.3 Enterprise Architecture (EA) Team

1. All FPIs are encouraged to set up in-house EA team that will:

    a. Assist the Management to ensure that all IT projects and initiatives are in compliance with the provisions of the NGEA;

    b. Provide timely advice to their Management on the need to carry out NGEA compliance assessments annually;

    c. Submit to Ne-GIF Governing Committee, a report on the status of NGEA compliance assessment carried out within their organization, on or before the stipulated 31st of January date through the Head of IT or e-Government; and

    d. Escalate challenges, suggestions, innovations and ambiguities etc. encountered in the process of implementing the NGEA to the NGEA Governing Committee through the Head of IT or e-Government.

2. The EA team should be made up of at least 5 persons to be drawn from both the IT and/or e-Government departments/units or EA unit.
3. The EA team should be headed by either the Head of e-Government or IT department/unit or EA unit
4. However, where an organization has both the Head of IT department/unit and Head of e-Government Department/unit but EA unit does not exist, the EA Team shall be co-chair by both. Where EA unit has been established, the head of EA unit shall head the EA Team. He/she shall be reporting to Head of IT and/or e-Government department.
5. Upon the creation of the EA Team, the details of its members should be communicated to the NGEA Governing Committee.
6. All communications from the EA Team to the NGEA Governing Committee shall be through the Head of the EA Team.

SECTION FIVE: Review and Updates

The fact that Information Technology keeps improving and public institutions' needs keep changing necessitate frequent review and update of NGEA to reflect the current circumstances. In view of this, there is need for the framework to be reviewed and updated (where necessary) from time to time.

The framework will be reviewed and updated biennially (i.e. every two years) or whenever there is an urgent need for review. The following shall be considered as urgent need:

1. Where it is observed and recommended by IT project clearance body of NITDA while performing its assignment that the provisions of the framework be reviewed and updated to reflect current requirements;
2. Where it is observed and recommended by the NGEA Governing Committee that key technical and/or non-technical provisions of the framework be reviewed and updated to accommodate current context;
3. Where any document(s) (international or local) relied on for the development of this framework has been substantially reviewed such that it affects the provisions of this framework; and
4. Where standards, specifications, methodologies, best practices, approaches etc. recommended in this framework have been substantially updated or discontinue and brought to the notice of the NGEA governing Committee.

Where a review is requested or has become necessary in line with any of the above requirements, the NGEA Governing Committee will:

1. Constitute a Sub-Committee to critically review the Framework and come up with a revised/updated draft;
2. The revised/updated draft will be presented to the NGEA Governing Committee for consideration and approval. The approved version will be presented to all stakeholders for further consideration, inputs and adoption;
3. Upon approval and adoption of such substantial review/update, the document shall be ratified by NGEA Governing Committee and published as the extant framework and labeled as a higher version of the NGEA i.e. 2.0, 3.0, 4.0 etc.
4. However, where the proposed review is minor and not likely to drastically affect the implementation of the framework, there will be no need to organize a stakeholders' meeting. Such minor alterations of the framework will upon approval by the NGEA Governing Committee be labeled as sub versions of the existing full version of the framework i.e. 1.1, 1.2 or 2.1, 2.2 etc.

Appendix

A.1

Customer Service Domain

Capabilities within this Customer Service Type are used to plan, schedule, and control the activities between the customer and the enterprise, both before and after a product or service is offered.

Table 11.0: A.1: Customer Service Domain

S/N	Service Domain	Service Type
1.	Customer Services	1. Customer Relationship Management 2. Customer Preferences 3. Customer Initiated Assistance

Customer Relationship Management Component

Service Component	Defines the set of capabilities to
Call Center Management	Handle telephone sales and/or service to the end customer
Customer Analytics	Allow for the analysis of an organization's customers, as well as the scoring of third-party information as it relates to an organization’s customers
Sales and Marketing	Facilitate the promotion of a product or service and capture of new business
Product Management	Facilitate the creation and maintenance of products and services
Brand Management	Support the application of a trade name to a product or service as well as developing an awareness for the name
Customer / Account Management	Support the retention and delivery of a service or product to an organization's clients
Contact and Profile Management	Provide a comprehensive view of all customer interactions, including calls, email, correspondence and meetings; also provides for the maintenance of a customer’s account, business and personal information

Partner Relationship Management	Provide a framework to promote the effective collaboration between an organization and its business partners, particularly members of the distribution chain (e.g., channel and alliance partners, resellers, agents, brokers, and dealers) and other third parties that support operations and service delivery to an organization’s customers; includes performance evaluation of partners, if necessary
Customer Feedback	Collect, analyze and handle comments and feedback from an organization's customers
Surveys	Collect useful information from an organization's customers

Customer Preferences Component

Capabilities within this Service Type allow an organization's customers to change a user interface and the way data is displayed.

Service Component	Defines the set of capabilities to
Personalization	Change a user interface and how data is displayed
Subscriptions	Allow a customer to join a forum, listserv, or mailing list
Alerts and Notifications	Allow a customer to be contacted in relation to a subscription or service of interest

Customer Initiated Assistance Component

Capabilities within this Service Type allow customers to proactively seek assistance and service from an organization.

Service Component	**Defines the set of capabilities to**
Online Help	Provide an electronic interface to customer assistance
Online Tutorials	Provide an electronic interface to educate and assist customers
Self-Service	Allow an organization's customers to sign up for a particular service at their own initiative
Reservations / Registration	Allow electronic enrollment and confirmations for services
Multi-Lingual Support	Allow access to data and information in multiple languages
Assistance Request	Support the solicitation of support from a customer
Scheduling	Define the set of capabilities that support the plan for performing work or service to meet the needs of an organization’s customers

Process Automation Component

The Process Automation Services Domain defines the set of capabilities supporting the automation of process and management activities to assist in effectively managing the business. The Process Automation Services domain represents those services and capabilities serving to automate and facilitate the processes associated with tracking, monitoring, and maintaining liaison throughout the business cycle of an organization.

2.	Process Automation	1. Tracking and Workflow 2. Routing and Scheduling

Tracking and Workflow

Capabilities within this Service Type provide automatic monitoring and routing of documents to the users responsible for working on them to support each step of the business cycle.

Service Component	**Defines the set of capabilities to**
Process Tracking	Allow the monitoring of activities within the business cycle
Case Management	Manage the life cycle of a particular claim or investigation within an organization to include creating, routing, tracing, assignment and closing of a case as well as collaboration among case handlers
Conflict Resolution	Support the conclusion of contention or differences within the business cycle

Routing and Scheduling

Capabilities within this Service Type provide automatic directing, assignment, or allocation of time for a particular action or event.

Service Component	**Defines the set of capabilities to**
Inbound Correspondence Management	Manage externally initiated communication between an organization and its stakeholders
Outbound Correspondence Management	Manage internally initiated communication between an organization and its stakeholders

Business Management Services Domain

The Business Management Services Domain defines the set of capabilities supporting the management of business functions and organizational activities to maintain continuity across the business and value-chain participants. The Business Management Services Domain represents those capabilities and services necessary for projects, programs and planning within a business operation to be successfully managed.

3.	Business Management Services	1. Management of Process 2. Organizational Management 3. Investment Management

		4. Supply Chain Management

Management of Process

Capabilities within this Service Type regulate the activities surrounding the business cycle of an organization.

Service Component	**Defines the set of capabilities to**
Change Management	Control the process for updates or modifications to the existing documents, software or business processes of an organization
Configuration Management	Control the hardware and software environments, as well as documents of an organization
Requirements Management	Gather, analyze and fulfill the needs and prerequisites of an organization's efforts
Program / Project Management	Manage and control a particular effort of an organization
Governance / Policy Management	Influence and determine decisions, actions, business rules and other matters within an organization
Quality Management	Help determine the level that a product or service satisfies certain requirements
Business Rule Management	Manage the enterprise processes that support an organization and its policies
Risk Management	Support the identification and probabilities or chances of hazards as they relate to a task, decision or long-term goal; includes risk assessment and risk mitigation

Organizational Management

Capabilities within this Service Type support both collaboration and communication within an organization.

Service Component	**Defines the set of capabilities to**
Workgroup / Groupware	Support multiple users working on related tasks
Network Management	Monitor and maintain a communications network in order to diagnose problems, gather statistics and provide general usage

Investment Management

Capabilities within this Service Type manage the financial assets and capital of an organization.

Service Component	**Defines the set of capabilities to**

Strategic Planning and Mgmt	Support the determination of long-term goals and the identification of the best approach for achieving those goals
Portfolio Management	Support the administration of a group of investments held by an organization
Performance Management	Measure the effectiveness of an organization's financial assets and capital

Supply Chain Management

Capabilities within this Service Type plan, schedule and control a supply chain and the sequence of organizations and functions to mine, make or assemble materials and products from manufacturer to wholesaler to retailer to consumer.

Service Component	**Defines the set of capabilities to**
Procurement	Support the ordering and purchasing of products and services
Sourcing Management	Support the supply of goods or services as well as the tracking and analysis of costs for these goods
Inventory management	Provide for the balancing of customer service levels with inventory investment

Digital Asset Services Domain

The Digital Asset Services Domain defines the set of capabilities to support the generation, management, and distribution of intellectual capital and electronic media across the business and extended enterprise.

Content Management

Capabilities within this Service Type manage the storage, maintenance and retrieval of documents and information of a system or website.

Service Component	**Defines the set of capabilities to**
Content Authoring	Allow for the creation of tutorials, CBT courseware, web sites,
Knowledge Distribution and Delivery	Support the transfer of knowledge to the end customer.
Smart Documents	Support the interaction of information and process (business logic) rules between users of the document. (i.e. the logic and use of the document is embedded within the document itself and is managed within the document parameters)

Records Management

Capabilities within this Service Type store, protect, archive, classify and retire documents and information.

Service Component	**Defines the set of capabilities to**
Record Linking / Association	Support the correlation between logical data and information sets

Document Classification	Support the categorization of documents and artifacts, both electronic and physical
Document Retirement	Support the termination or cancellation of documents and artifacts used by an organization and its stakeholders
Digital Rights Management	Support the claim and ownership of intellectual capital and artifacts belonging to an organization

Business Analytical Services Domain

The Business Analytical Services Domain defines the set of capabilities supporting the extraction, aggregation, and presentation of information to facilitate decision analysis and business evaluation.

Analysis and Statistics

Capabilities within this Service Type examine business issues, problems and their solutions.

Service Component	**Defines the set of capabilities to**
Mathematical	Support the formulation and mathematical analysis of probabilistic models for random phenomena and the development and investigation of methods and principles for statistical inference
Structural / Thermal	Support the use of data flow and data modeling diagrams for applying systematic analysis of data
Radiological	Support the use of radiation and x-ray technologies for analysis and scientific examination
Forensics	Support the analysis of physical elements using science and technology for investigative and legal purposes

Visualization

Capabilities within this Service Type convert data into graphical or picture form

Service Component	**Defines the set of capabilities to**
Graphing / Charting	**Support the presentation of information in the form of diagrams or tables**
Imagery	**Support the creation of film or electronic images from pictures or paper forms**
Multimedia	**Support the representation of information in more than one form to include text, audio, graphics, animated graphics and full motion video**
Mapping / Geospatial / Elevation / GPS	**Provide for the representation of position information through the use of attributes such as elevation, latitude, and longitude coordinates**
CAD	**Support the design of products with computers**

Knowledge Discovery

Capabilities within this Service Type facilitate the identification of useful information from data

Service Component	**Defines the set of capabilities to**
Data Mining	Provide for the efficient discovery of non-obvious, valuable patterns and relationships within a large collection of data
Modeling	Develop descriptions to adequately explain relevant data for the purpose of prediction, pattern detection, exploration or general organization of data
Simulation	Utilize models to mimic real-world processes

Business Intelligence

Capabilities within this Service Type provide information pertaining to the history, current status or future projections of an organization.

Service Component	**Defines the set of capabilities to**
Demand Forecasting / Mgmt	Facilitate the prediction of sufficient production to meet an organization's sales of a product or service
Balanced Scorecard	Support the listing and analyzing of both positive and negative impacts associated with a decision

Decision Support and Planning	Support the analysis of information and predict the impact of decisions before they are made

Reporting

Capabilities within this Service Type organize data into useful information.

Service Component	Defines the set of capabilities to
Ad Hoc	Support the use of dynamic reports on an as needed basis
Standardized / Canned	Support the use of pre-conceived or pre-written reports
OLAP	Support the analysis of information that has been summarized into multidimensional views and hierarchies

Back Office Services Domain

The Back Office Services Domain defines the set of capabilities supporting the management of enterprise planning and transactional-based functions.

Service Component	Defines the set of capabilities to
Data Exchange	Support the interchange of information between multiple systems or applications; includes verification that transmitted data was received unaltered
Data Mart	Support a subset of a data warehouse for a single department or function within an organization
Data Warehouse	Support the archiving and storage of large volumes of data
Meta Data Management	Support the maintenance and administration of data that describes data
Data Cleansing	Support the removal of incorrect or unnecessary characters and data from a data source
Extraction and Transformation	Support the manipulation and change of data
Loading and Archiving	Support the population of a data source with external data
Data Recovery	Support the restoration and stabilization of data sets to a consistent, desired state
Data Classification	Allow the classification of data

Human Resources

Capabilities within this Service Type provide for the recruitment and management of personnel

Service Component	Defines the set of capabilities to
Recruiting	Support the identification and hiring of employees for an organization
Resume Management	Support the maintenance and administration of one's professional or work experience and qualifications
Career Development and Retention	Support the monitoring of performance as well as the professional growth, advancement, and retention of an organization's employees
Time Reporting	Support the submission, approval and adjustment of an employee's hours
Awards Management	Support the recognition of achievement among employees of an organization
Benefit Management	Support the enrollment and participation in an organization's compensation and benefits programs
Retirement Management	Support the payment of benefits to retirees
Personnel Administration	Support the matching between an organization’s employees and potential opportunities as well as the modification, addition and general upkeep of an organization’s employee-specific information
Education / Training	Support the active building of employee competencies, to
Health and Safety	Support the security and physical well-being of an organization's employees
Travel Management	Support the transit and mobility of an organization's employees for business purposes

Financial Management

Capabilities within this Service Type provide the accounting practices and procedures to allow for the handling of revenues, funding and expenditures.

Service Component	Defines the set of capabilities to
Billing and Accounting	Support the charging, collection and reporting of an organization's accounts
Credit / Charge	Support the use of credit cards or electronic funds transfers for payment and collection of products or services
Expense Management	Support the management and reimbursement of costs paid by employees or an organization
Payroll	Involve the administration and determination of employees compensation
Payment / Settlement	Support the process of accounts payable
Debt Collection	Support the process of accounts receivable
Revenue Management	Support the allocation and re-investment of earned net credit or capital within an organization

Internal Controls	Support the methods and procedures used by the organization to safeguard its assets, produce accurate accounting data and reports, contribute to efficient operations, and encourage staff to adhere to management policies and mission requirements
Auditing	Support the examination and verification of records for accuracy
Activity-Based Management	Support a defined, specific set of finance-related tasks for a given objective
Currency Translation	Support the calculations and difference between multiple mediums of exchange

Assets / Materials Management

Capabilities within this Service Type support the acquisition, oversight and tracking of an organization's assets

Service Component	**Defines the set of capabilities to**
Property / Asset Management	Support the identification, planning and allocation of an organization's physical capital and resources
Asset Cataloging / Identification	Support the listing and specification of available assets
Asset Transfer, Allocation, and Maintenance	Support the movement, assignment, and replacement of assets
Facilities Management	Support the construction, management and maintenance of facilities for an organization
Computers / Automation Management	Support the identification, upgrade, allocation and replacement of physical devices, including servers and desktops, used to facilitate production and process-driven activities

Development and Integration

Capabilities within this Service Type provide communication between hardware/software applications and the activities associated with deployment of software applications.

Service Component	**Defines the set of capabilities to**
Legacy Integration	Support the communication between newer generation hardware/software applications and the previous, major generation of hardware/software applications
Enterprise Application Integration	Support the redesigning of disparate information systems into one system that uses a common set of data structures and rules
Data Integration	Support the organization of data from separate data sources into a single source using middleware or application integration as well as the modification of system data models to capture new information within a single system

Instrumentation and Testing	Support the validation of application or system capabilities and requirements
Software Development	Support the creation of both graphical and process application or system software

Human Capital / Workforce Management

Capabilities within this Service Type provide for the planning and supervision of an organization's personnel

Service Component	**Defines the set of capabilities to**
Resource Planning and Allocation	Support the determination of strategic direction, the identification and establishment of programs and processes, and the allocation of resources (capital and labor) among those programs and processes
Skills Management	Support the proficiency of employees in the delivery of an organization's products or services
Workforce Directory / Locator	Support the listing of employees and their whereabouts
Team / Org Management	Support the hierarchy structure and identification of employees within the various sub-groups of an organization
Contingent Workforce Management	Support the continuity of operations for an organization's business through the identification of alternative organization personnel
Workforce Acquisition / Optimization	Support the hiring and re-structuring of employees and their roles within an organization

Support Services Domain

The Support Services Domain defines the set of cross-functional capabilities able to be leveraged independent of Service Domain objective and/or mission.

Security Management

Capabilities within this Service Type protect an organization's information and information systems.

Service Component	**Defines the set of capabilities to**
Identification and Authentication	Support obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users
Access Control	Support the management of permissions for logging onto a computer, application, service, or network; includes user management and role/privilege management

Cryptography	Support the use and management of ciphers, including encryption and decryption processes, to ensure confidentiality and integrity of data
Digital Signature Management	Use and management of electronic signatures to support authentication and data integrity; includes public key infrastructure (PKI)
Intrusion Prevention	Perform penetration testing and other measures to prevent unauthorized access to a government information system
Intrusion Detection	Support the detection of unauthorized access to a government information system
Incident Response	Provide active response and remediation to a security incident that has allowed unauthorized access to a government information system
Audit Trail Capture and Analysis	Support the identification and monitoring of activities within an application, system, or network
Certification and Accreditation	Support the certification and accreditation (C&A) of federal information systems, as described in NIST SP800-37.
FISMA Management and Reporting	Support management and reporting of compliance with the Federal Information Security Management Act of 2002
Virus Protection	Provide anti-virus service to prevent, detect, and remediate infection of government computing assets

Collaboration

Capabilities within this Service Type allow for the concurrent, simultaneous communication and sharing of content, schedules, messages and ideas within an organization

Service Component	**Defines the set of capabilities to**
Email	Support the transmission of memos and messages over a network
Threaded Discussions	Support the running log of remarks and opinions about a given topic or subject
Document Library	Support the grouping and archiving of files and records on a server
Shared Calendaring	Allow an entire team as well as individuals to view, add and modify each other’s schedules, meetings and activities
Task Management	Support a specific undertaking or function assigned to an employee

Search

Capabilities within this Service Type provide for the probing and lookup of specific data from a data source.

Service Component	Defines the set of capabilities to
Query	Support retrieval of records that satisfy specific query selection criteria
Precision / Recall Ranking	Support selection and retrieval of records ranked to optimize precision against recall
Classification	Support selection and retrieval of records organized by shared characteristics in content or context
Pattern Matching	Support retrieval of records generated from a data source by imputing characteristics based on patterns in the content or context

Communication

Capabilities within this Service Type transmit data, messages and information in multiple formats and protocols.

Service Component	Defines the set of capabilities to
Real Time / Chat	Support the conferencing capability between two or more users on a local area network or the internet
Instant Messaging	Support keyboard conferencing over a Local Area Network or the internet between two or more people
Audio Conferencing	Support audio communications sessions among people who are geographically dispersed
Video Conferencing	Support video communications sessions among people who are geographically dispersed
Event / News Management	Monitor servers, workstations and network devices for routine and non-routine events
Community Management	Support the administration of online groups that share common interests
Computer / Telephony Integration	Support the connectivity between server hardware, software and telecommunications equipment into a single logical system
Voice Communications	Provide telephony or other voice communications

Systems Management

Capabilities within this Service Type support the administration and upkeep of an organization’s technology assets, including the hardware, software, infrastructure, licenses, and components that comprise those assets.

Service Component	Defines the set of capabilities to
License Management	Support the purchase, upgrade and tracking of legal usage contracts for system software and applications
Remote Systems Control	Support the monitoring, administration and usage of applications and enterprise systems from locations outside of the immediate system environment
System Resource Monitoring	Support the balance and allocation of memory, usage, disk space and performance on computers and their applications
Software Distribution	Support the propagation, installation and upgrade of written computer programs, applications and components
Issue Tracking	Receive and track user-reported issues and problems in using IT systems, including help desk calls

Forms Management

Capabilities within this Service Type support the creation, modification, and usage of physical or electronic documents used to capture information within the business cycle.

Service Component	Defines the set of capabilities to
Forms Creation	Support the design and generation of electronic or physical forms and templates for use within the business cycle by an organization and its stakeholders
Forms Modification Optimization	Support the maintenance of electronic or physical forms, templates and their respective elements and fields roles within an organization

A.2

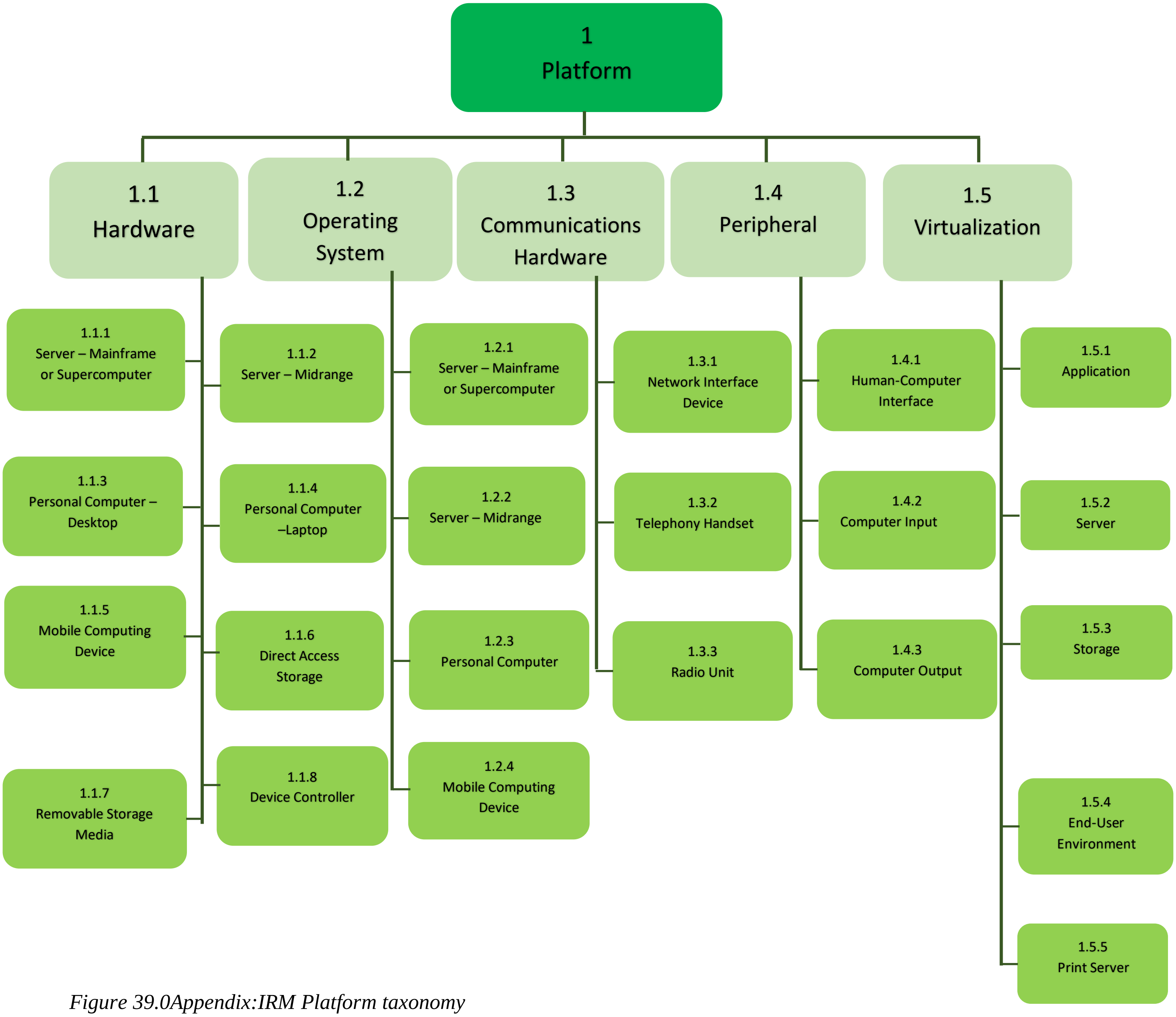


Figure 39.0Appendix:IRM Platform taxonomy

Table 12.0: Table A.2: 1.1 Hardware

Code	Domain	Area	Category	Definition
1.1	Platform	Hardware		Hardware, in a computer context, refers to the physical components that make up a computer system, including the basic machine itself.

				There are many different kinds of machines and different kinds of hardware that can be installed inside, and connected to the outside, of a computer.
1.1.1	Platform	Hardware	Server - Mainframe or Supercomputer	A Server is a computer that provides data to other computers. It may serve data to systems on a Local Area Network (LAN) or a Wide Area Network (WAN) over the Internet. A Mainframe is a high-performance computer used for large-scale computing purposes that require greater availability and security. It often serves many connected terminals and is usually used by large complex organizations. A supercomputer is a high-performance computing machine designed to have extremely fast processing speeds. Supercomputers have various applications, such as performing complex scientific calculations, modeling simulations, and rendering large amounts of 3D graphics. The chief difference between a supercomputer and a mainframe is that a supercomputer channels all its power into executing a few programs as fast as possible, whereas a mainframe uses its power to execute many programs concurrently.
1.1.2	Platform	Hardware	Server - Midrange	A midrange computer is a medium-sized computer system or server. Midrange computers encompass a very broad range and reside in capacity between high-end PCs and mainframes. Formerly called "minicomputers", which were hosts to dumb terminals connected over dedicated cables, most midrange computers today function as servers in a network.
1.1.3	Platform	Hardware	Personal Computer-Desktop	A desktop computer is a personal computer in a form intended for regular use at a single location, as opposed to a mobile laptop or portable computer. A Personal Computer (PC) is any general-purpose computer whose size, capabilities, and original sales price make it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator.

1.1.4	Platform	Hardware	Personal Computer-Laptop	A laptop computer is a personal computer for mobile use. A Personal Computer (PC) is any general-purpose computer whose size, capabilities, and original sales price make it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. A laptop integrates most of the typical components of a desktop computer, including a display, a keyboard, a pointing device such as a touchpad and speakers into a single unit.
1.1.5	Platform	Hardware	Mobile Computing Device	A mobile computing device is a small, hand-held computing device, typically having a display screen with touch input and/or a miniature keyboard. Such devices have an Operating System (OS), and can run various types of application software, known as apps. Most devices can also be equipped with WI-FI, Bluetooth, GPS and more capabilities that can allow connections to the Internet, other Bluetooth or smart capable devices such as a laptop or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.
1.1.6	Platform	Hardware	Direct Access Storage	Direct access storage device is a general term for magnetic disk storage devices and solid state storage devices. Within the IRM, the term refers to magnetic storage devices for mainframes, midranges, and PCs. "Direct access" means that all data can be accessed directly in about the same amount of time, rather than having to progress sequentially through the data.
1.1.7	Platform	Hardware	Removable Storage Media	Removable storage media is any type of storage device that can be removed from a computer while the system is running.
1.1.8	Platform	Hardware	Device Controller	A device controller is a part of a computer system that makes sense of the signals going to and coming from the CPU.

Table 13.0: A.2: 1.2 Operating System

1.2	Platform	Operating System		An Operating System (OS) is a computer program, implemented in either software or firmware, which acts as an intermediary between users of a computer and the computer hardware. The purpose of an operating system is to provide an environment in which a user can execute applications.
1.2.1	Platform	Operating System	Server - Mainframe or Supercomputer	A mainframe or supercomputer operating system is, in simplest terms, a collection of programs that manage a computer system's internal workings - its memory, processors, devices, and file system. Mainframe operating systems are tailored to meet the substantially different architectures and purposes of mainframes as high-volume transaction processing devices, or the purposes of supercomputers as high-volume algorithmic processors.
1.2.2	Platform	Operating System	Server - Midrange	A midrange computer operating system is, in simplest terms, a collection of programs that manage a computer system's internal workings - its memory, processors, devices, and file system. Midrange computers are almost universally known as servers to recognize that they often "serve" applications to end users at "client" computers, that they use a client/server computing model.
1.2.3	Platform	Operating System	Personal Computer	For personal computers, operating systems are generally tailored to the needs of users on standalone machines that may or may not connect to a network, and are generally not servers of information to large numbers of other machines.
	Platform	Operating System	Mobile Computing Device	As with other operating systems, a mobile computing device Operating System (OS) is a computer program, implemented in either software or firmware, which acts as an intermediary between users of a computer and the computer hardware. The purpose of an OS is to provide an environment in which a user can execute applications.

Table 14.0: A.2, 1.3: Communication Hardware

1.3	Platform	Communications Hardware		Communications Hardware refers broadly to hardware intended primarily to create a link to the network from the user or another computational
1.3.1	Platform	Communications Hardware	Network Interface Device	For the purposes of the IRM, a Network Interface Device is a broad term that includes devices that serve as a demarcation point between the carrier's
1.3.2	Platform	Communications Hardware	Telephony Handset	A telephony handset is a device the user holds to the ear to hear the audio sound, usually containing the phone's microphone.
1.3.3	Platform	Communications Hardware	Radio Unit	A Radio unit is a device that transmits signals through free space by electromagnetic waves with frequencies significantly below visible

Table 15.0: A.2, 1.4: Peripheral

1.4	Platform	Peripheral	A peripheral is a device connected to a host computer, but not part of it. It expands the host's capabilities but does not form part of the core computer architecture. It is often, but not always, partially or completely dependent on the host. Usually, the word peripheral is used to refer to a device external to the computer case, but the devices located inside the computer case (particularly with laptops) are also technically peripherals. Devices that exist outside the computer case are called external peripherals, or auxiliary components. Devices that are inside the case such as internal hard drives or CD-ROM drives are also peripherals in technical terms and are called internal peripherals, but may not be recognized as peripherals by laypeople. For the purposes of the IRM, three different types of peripherals are recognized: Human-Computer Interface, Computer Input, and Computer Output. Storage devices, commonly a form of peripheral, are handled in virtualization.

1.4.1	Platform	Peripheral	Human-Computer Interface	The human-computer interface can be described as the point of communication between the human user and the computer, and, as such, all devices that primarily facilitate such ongoing interactions are grouped here.
1.4.2	Platform	Peripheral	Computer Input Device	Inputs are the signals or data received by the system, and outputs are the signals or data sent from it. For the purposes of the IRM, computer input devices are those that provide data to the machine/application combination for further processing or for manipulation by users through the human- computer interface devices.
1.4.3	Platform	Peripheral	Computer Output Device	Inputs are the signals or data received by the system, and outputs are the signals or data sent from it. For the purposes of the IRM, computer output devices are those that provide data from the machine/application combination to other machines or to the user for asynchronous consumption.

Table 16.0:A.2, 1.5:Virtualization

1.5	Platform	Virtualization	In computing, virtualization is the creation of a virtual (rather than actual) version of something, such as a hardware platform, Operating System (OS), storage device, or network resources. This section of the IRM categorizes those mechanisms to create virtual platforms.

1.5.1	Platform	Virtualization	Application	For the purposes of the IRM, application virtualization encapsulates application from the underlying operating system on which they are executed. A fully virtualized application is not installed in the traditional sense, although it is still executed as if it were. The application is fooled at runtime into believing that it is directly interfacing with the original operating system and all the resources managed by it, when in reality it is not. In this context, the term "virtualization" refers to the artifact being encapsulated (application), which is quite different to its meaning in hardware virtualization, where it refers to the artifact being abstracted (physical hardware).
1.5.2	Platform	Virtualization	Server	Virtual servers are virtual machines where each server, although running in software on the same physical computer as other customers' servers, is in many respects functionally equivalent to a separate physical computer. A virtual server is dedicated to the individual customer's needs, has the privacy of a separate physical computer, and is configured to run server software. The term cloud server is also used to describe the same concept, normally where such systems can be setup and re-configured on the fly.
1.5.3	Platform	Virtualization	Storage	Storage virtualization applies virtualization concepts to enable better functionality and more advanced features within the storage system. Storage systems use special hardware and software along with disk drives in order to provide very fast and reliable storage for computing and data processing.
1.5.4	Platform	Virtualization	End-User Environment	End-User Environment virtualization is a broad term including desktop and client virtualization. End-User virtualization separates a personal computer desktop or mobile computing environment from a physical machine using the client-server model of computing.

1.5.5	Platform	Virtualization	Print Server	Print server virtualization extends the virtualization concept to the access to and management of print resources. For the purposes of the IRM, a print server can be a dedicated device, a standalone computer, specialized software, or some combination that handles receipt, queuing, delivery, and status of print jobs for printers on the network.

A.2 Network Domain

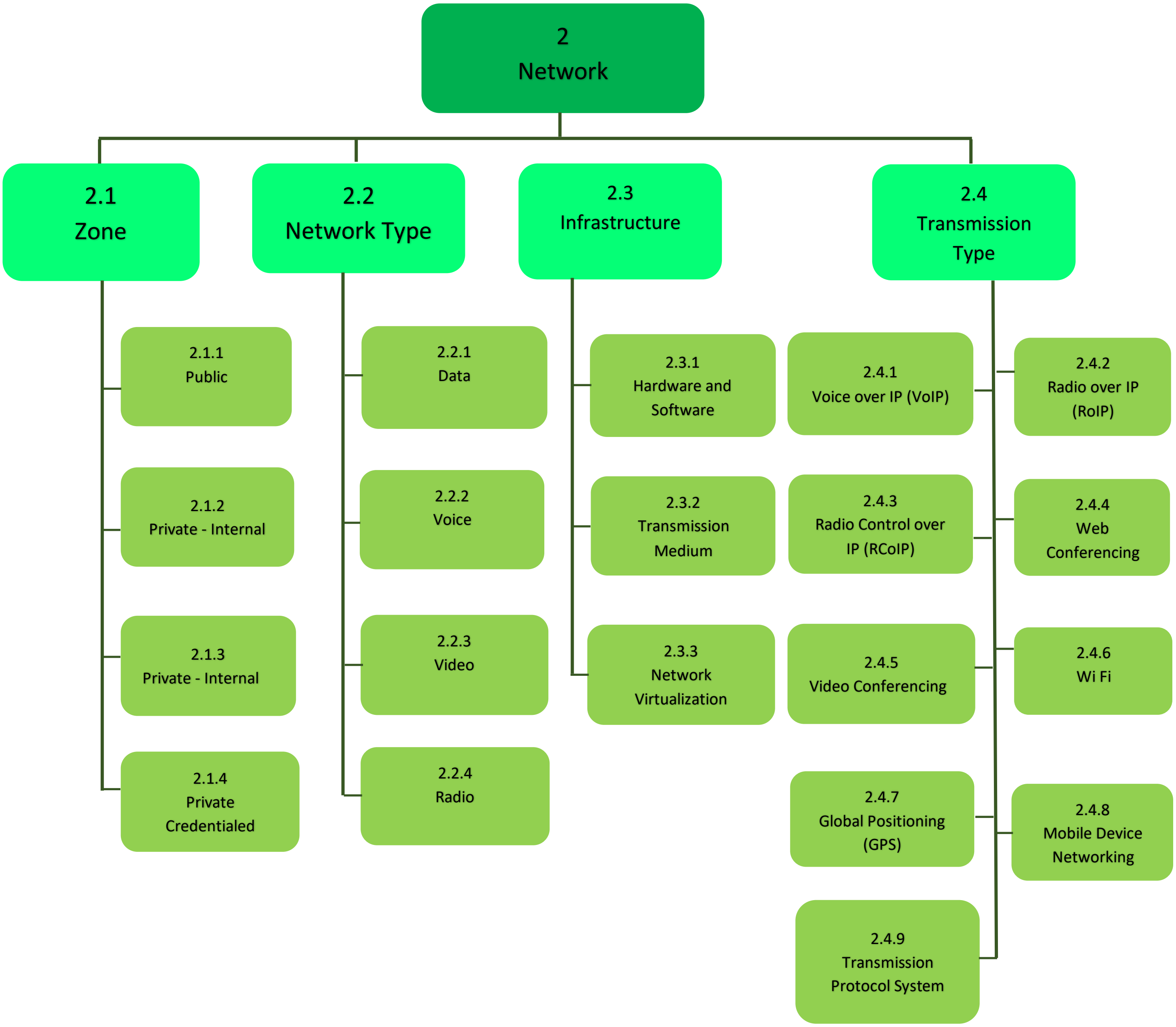


Figure 40.0: A.2: IRM Network Domain

Table 17.0: A.2, 2.1:Zone

Code	Domain	Area	Category	Definitions
2.1	Network	Zone		For the purposes of the IRM, a Zone is a conceptual division of the network into areas that are separated (usually by security measures) from one another.
2.1.1	Network	Zone	Public	Assets in the public zone are accessible to anyone, without credentials, from outside the boundaries of the organization.
2.1.2	Network	Zone	Private - Internal	Assets in the private, internal zone are accessible only from within the boundaries of a single organization
2.1.3	Network	Zone	Private - Shared	Assets in the private, shared zone are accessible to more than one major organization, but only within the boundaries of those participating organizations.
2.1.4	Network	Zone	Private - Credentialed	Assets in the private, credentialed zone are accessible only with appropriate credentials from outside the boundaries of the organization.

Table 18.0: A.2, 2.2:Network Type

2.2	Network	Network Type	For the purposes of the IRM, a Network Type categorizes the major types of traffic on a given network. A single network may carry more than one type of traffic.

2.2.1	Network	Network Type	Data	A data network type is an electronic communications process that allows for the orderly transmission and receptive of data, such as letters, spreadsheets, and other types of documents. What sets the data network apart from other forms of communication, such as an audio network, is that the data network is configured to transmit data only. This is in contrast to the audio or voice network, which is often employed for both voice communications and the transmission of data such as a facsimile transmission.
2.2.2	Network	Network Type	Voice	Voice networks are sometimes dedicated, as in the original public switched telephone network (PSTN), but have changed to be a type of traffic carried on data networks using some form of packet-switching technology. Voice traffic is distinct from Data traffic in the delivery requirements (it needs to arrive nearly synchronously and be assembled in order without drop-outs) and bandwidth usage (which is high).
2.2.3	Network	Network Type	Video	Video networks can be dedicated links devoted to video for large video conferencing installations. As with Voice traffic, Video is often a type of traffic carried on data networks using some form of packet-switching technology. Video traffic is distinct from Data traffic in the delivery requirements (it needs to arrive nearly synchronously and be assembled in order without drop-outs) and bandwidth usage (which is very high).
2.2.4	Network	Network Type	Radio	Radio networks are transmitted through free space by radio waves. There are two types of radio networks currently in use around the world: the one-to- many broadcast network commonly used for public information and mass media entertainment; and the two-way type used more commonly for public safety and public services such as police, fire, taxicabs, and delivery services. Many of the same components and much of the same basic technology applies to both.

Table 19.0: A.2, 2.3:Infrastructure

2.3	Network	Infrastructure	For the purposes of the IRM, Infrastructure, as used here, is a broad term covering the various forms of basic hardware and software that comprise the foundation of a network.

2.3.1	Network	Infrastructure	Hardware and Software	Specifically, for Networks, Hardware and Software refers to many different kinds of devices and their firmware. These devices provide many things including routing, security, etc. The software included here is the firmware and/or Operating System (OS) associated with specific network devices.
2.3.2	Network	Infrastructure	Transmission Medium	Transmission medium is the material and/or technology that carries signal from one location to another.
2.3.3	Network	Infrastructure	Network Virtualization	A virtual network is a computer network that consists, at least in part, of virtual network links. A virtual network link is a link that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. The two most common forms of network virtualization are protocol-based virtual networks (such as Virtual Local Area Networks (VLAN), Virtual Private Networks (VPN), and Virtual Private LAN Services (VPLS)) and virtual networks that are based on virtual devices (such as the networks connecting virtual machines inside a hypervisor).

Table 20.0: A.2, 2.4:Transmission Medium

2.4	**Network**	**Transmission Type**	The Transmission Type category allows for identification of the low-level infrastructure "applications" that form the core of the network,

2.4.1	Network	Transmission Type	Voice over IP (VoIP)	Voice over IP (VoIP, or Voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, Voice over Broadband (VoBB), broadband telephony, IP communications, and broadband phone. Internet telephony refers to communications services — voice, fax, SMS, and/or voice-messaging applications — that are transported via the Internet, rather than the Public Switched Telephone Network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP Telephony and VoIP are terms that are used interchangeably, they are actually different; IP telephony has to do with digital telephony systems that use IP protocols for voice communication, while VoIP is actually a subset of IP Telephony. VoIP is a technology used by IP telephony as a means of transporting phone calls.

2.4.2	Network	Transmission Type	Radio over IP (RoIP)	Radio over Internet Protocol (RoIP) is similar to VoIP, but augments two-way radio communications rather than telephone calls. From the system point of view, it is essentially VoIP with PTT (Push To Talk). To the user it can be implemented like any other radio network. With RoIP, at least one node of a network is a radio (or a radio with an IP interface device) connected via IP to other nodes in the radio network. The other nodes can be two-way radios, but could also be dispatch consoles either traditional (hardware) or modern (software on a PC), POTS telephones, softphone applications running on a computer such as a Skype phone, PDA, smartphone, or some other communications device accessible over IP. RoIP can be deployed over private networks as well as the public Internet.
2.4.3	Network	Transmission Type	Radio Control over IP (RCoIP)	Radio Control over Internet Protocol (RCoIP) builds on the concepts of RoIP, but can be used in combination with analog radio units. In RCoIP, handsets and other mobile units are remotely controlled using IP-delivered commands.
2.4.4	Network	Transmission Type	Web Conferencing	Web conferencing refers to a service that allows conferencing events to be shared with remote locations. In general the service is made possible by Internet technologies, particularly on TCP/IP connections. The service allows real-time point-to-point communications as well as multicast communications from one sender to many receivers. It offers information of text-based messages, voice and video chat to be shared simultaneously, across geographically dispersed locations.
2.4.5	Network	Transmission Type	Video Conferencing	Videoconferencing is the conduct of a videoconference (also known as a video conference or video teleconference) by a set of telecommunication technologies which allow two or more locations to communicate by

2.4.6	Network	Transmission Type	Wi-Fi	Wi-Fi (/'waifai/, also spelled Wifi or WiFi) is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards". However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN".
2.4.7	Network	Transmission Type	Global Positioning System (GPS)	The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather, anywhere on or near the Earth, where there is an unobstructed line of sight to four or more GPS satellites. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver.
2.4.8	Network	Transmission Type	Mobile Device Networking	Mobile Device Networking covers the sets of standards commonly used for mobile devices and mobile telecommunication services and networks that comply with specifications by the International Telecommunication Union. Such standards find applications in wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV, among others.
2.4.9	Network	Transmission Type	Transmission Protocol	Transmission Protocol is a category that allows grouping and identification of various transmission standards, at a basic level in the OSI stack.

‘

A.2 Facility Domain

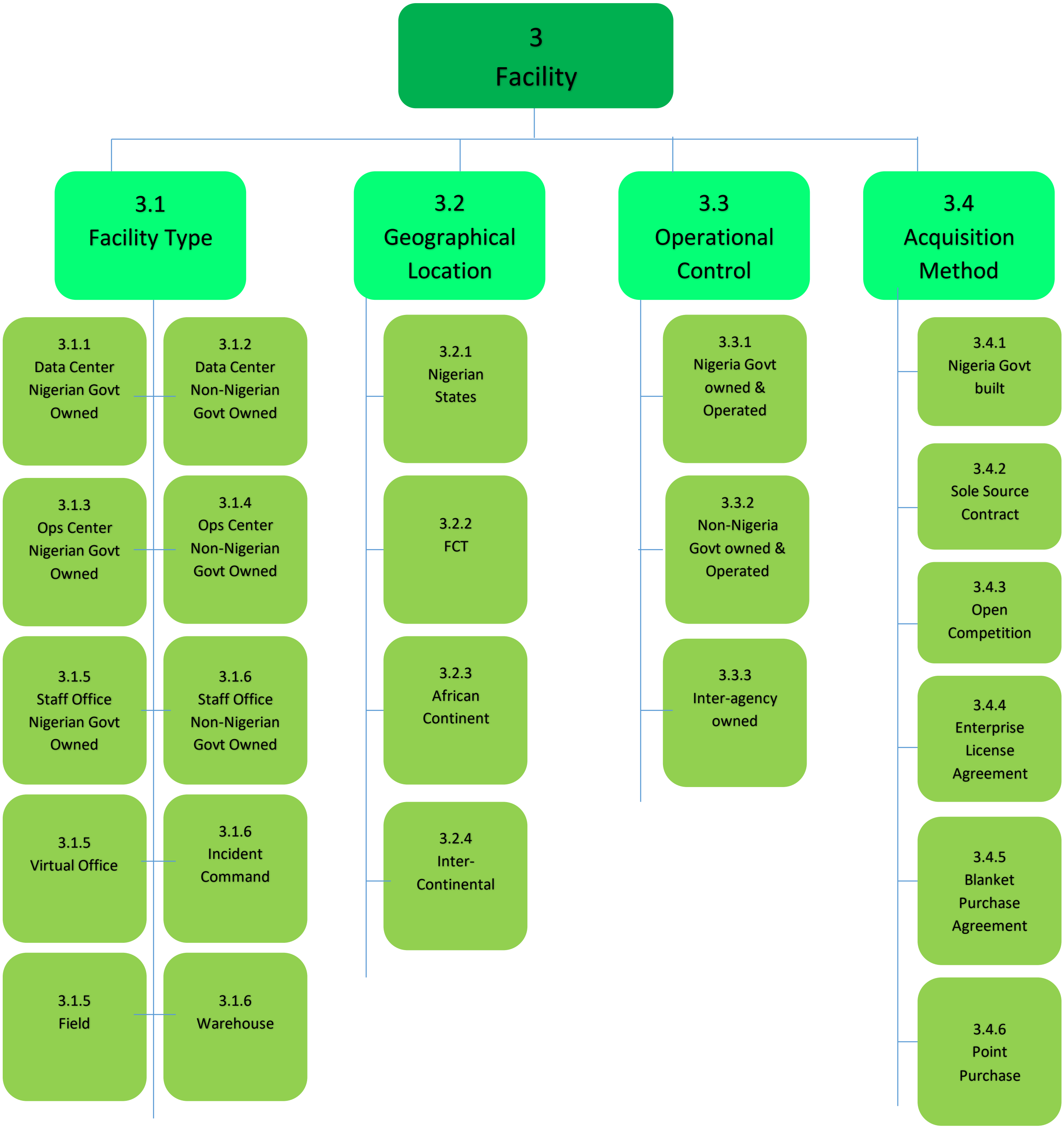


Figure 41.0: A.2 IRM Facility Domain

Table 21.0: A.2: Facility Domain

Code	Domain	Area	Category	Definition
3.1	Facility	Facility Type		The particular kind of location in which the assets are deployed.
3.1.1	Facility	Facility Type	Data Center – Nigerian Govt Owned	A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. In this instance, such operations center would be the primary responsibility of the Nigerian Government or Nigerian Government owned company , with or without contract support.
3.1.2	Facility	Facility Type	Data Center – Non Nigerian Govt Owned	The same as 3.1.1 but owned by private enterprise. These are enterprises with large networks as well as service providers may use a third- party data center to shift the burden of data center operations onto the third party, with or without direct support of Nigerian Government employees.

3.1.3	Facility	Facility Type	Operations Center - Nigerian Govt Owned	An operations center is designed to monitor IT assets deployed elsewhere on an enterprise network. There are many different kinds of operations centers, including "Network Operations Center" (NOC) and "Security Operations Center" (SOC). In this instance, such operations center would be the primary responsibility of the Nigerian Government, with or without contract support.
3.1.4	Facility	Facility Type	Operations Center - Non-Nigerian Govt Owned	Same as above in 3.2.3 but owned by private enterprise These enterprises with large networks as well as service providers may use a third-party operations center to shift the burden of operational monitoring onto the third party, with or without direct support of Nigerian Government employees.
3.1.5	Facility	Facility Type	Staff Office - Nigerian Govt Owned	For the purposes of the IRM, a staff office is any physical location/building intended to be a destination for actual individuals to regularly report for work functions, including locations primarily devoted to research, development, and/or science. In this instance, such staff offices would be the primary responsibility of the Nigerian Government, with or without the addition of contract staff.

3.1.6	Facility	Facility Type	Staff Office - Non- Nigerian Govt Owned	Same as 3.1.5 but owned by private enterprise. In this instance, such staff offices would be the primary responsibility of a third party, where Nigerian Government employees may or may not be stationed.
3.1.7	Facility	Facility Type	Virtual Office	For the purposes of the IRM, a Virtual Office is a workspace not set in a specific geographic location, but rather connected (via the Internet) to the wider enterprise. Virtual Offices include telework arrangements for Nigerian Government employees (when they are off-site), contract staff that works remotely, or some combination.
3.1.8	Facility	Facility Type	Incident Command	For the purposes of the IRM, an Incident Command includes smaller, often temporary locations for the management of forward operations or crisis / emergency management. It can be set up by security operators and/or national emergency agencies.
3.1.9	Facility	Facility Type	Field	For the purposes of the IRM, the Field includes any active deployment outside of traditional staff facilities, including anything from the battlefield to on-site research and data-gathering.
3.1.10	Facility	Facility Type	Warehouse	For the purposes of the IRM, Warehouse covers any place in which IT assets are stored or staged. The storage or staging may be for any purpose, including, but not limited to delivery to an eventual service location, disposal, or further decisions. The intent of this category is to identify IT assets not currently in active use.

Table 22.0: A.3: Purpose

Code	Area	Considerati	Context	Definition
Sec 1.1	Purpose	Regulatory Conditions		The regulatory conditions levied on an information system are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Sec. 1.1.1	Purpose	Regulatory Condition	Public Law	Public laws applicable to all government agencies regarding IT security.
Sec. 1.1.2	Purpose	Regulatory Conditions	National regulations and/or guidance	Any security-related regulation and/or guidance issued at Federal level by specific government body responsible for such, that adds to or interprets IT security standards, policies, laws and regulations.
Sec.1.1.3	Purpose	Regulatory Conditions	Executive Orders, strategy/plan	Executive Orders, security directives regarding classification and protection of information or other security goals.
Sec.1.1.4	Purpose	Regulatory Conditions	International Standards	Mandatory and recommended security standards such as ISO/IEC 27001, ETSI cyber security and ANSI/ISA 62443 etc.
Sec.1.1.4	Purpose	Regulatory Conditions	Organization Guidance	Any security-related guidance issued at an organization level that adds to or interprets federal standards, policies, laws and regulations.

Code	Area	Consideration	Context	Definition

Sec 1.2	Purpose	Risk Profile		Risk is the probability of a vulnerability being exploited, multiplied by the impact resulting from that vulnerability being exploited. Types of risk include: program or acquisition risk (e.g., cost, schedule, performance); compliance and regulatory risk); financial risk; legal risk; operational (e.g., mission or business) risk; political risk; project risk; reputational risk; safety risk; strategic planning risk; and supply chain risk.
Sec 1.2.1	Purpose	Risk Profile	Threat	It refers to anything that has the potential to cause serious harm to a computer system. The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. E.g. NIST SP 800-37
Sec 1.2.2	Purpose	Risk Profile	Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. E.g. NIST SP 800-37.

Table 23.0: A.3 Risk

Code	Area	Consideration	Context	Definition
2.1	Risk	Risk Assessment Processes		Risk assessment processes are used to determine the risk to the business of government within the context of a program or IT system, the level of acceptable risk, and corresponding controls that would best reduce the risk to acceptable levels through preventative measures.

2.1.1	Risk	Risk Assessment Processes	Impact Analysis	The process to identify potential impacts that could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. See NIST 800-60, ISO/IEC 27001, ETSI cyber security and ANSI/ISA 62443 etc.
2.1.2	Risk	Risk Assessment Processes	Security Objective Determination	This involves all functions pertaining to the protection of public institutions information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction.
2.1.3	Risk	Risk Assessment Processes	Align Preventative Measures	The protective measures prescribed to meet the security requirements (e.g., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. See NIST SP 800-53, NIST SP 800-37, ISO/IEC 27001, ETSI cyber security and ANSI/ISA 62443 etc.
2.1.4	Risk	Risk Assessment Processes	Control Selection	The minimum security countermeasures to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. See NIST SP 800-53, NIST SP 800-37, and ISO/IEC 27001, ETSI cyber security and ANSI/ISA 62443 etc

2.1.5	Risk	Risk Assessment Processes	Continuous Monitoring	The monitoring activities required to determine the effectiveness of security controls and the extent to which they comply with related laws, regulations, and policies.
2.2	Risk	Impact Mitigation		Impact mitigation considers the activities needed to reduce the impact to the organization when vulnerability is exploited.
2.2.1	Risk	Preparation		The preparatory measures to ensure that an organization can respond effectively to security incidents. See NIST SP 800-61, NIST SP 800-83 and ISO/IEC 27001
2.1.2	Risk	Detection and Analysis		The capability needed to detect, validate, and assess impact and prioritize response to security incidents. See NIST SP 800-61
2.1.3	Risk	Containment, Eradication and Recovery		The activities needed to contain, eradicate and recover from a security incident, including documenting evidence, mitigation of exploits, elimination of vulnerability, and confirmation of normal operating functionality. See NIST SP 800-61 and ISO/IEC 27001
2.2.4	Risk	Post Incident Activity and Notification		The process of conducting a robust assessment of lessons learned after incidents, identifying needed changes to security policy, and providing adequate reporting of all incidents. See NIST SP 800-61 and ISO/IEC 27001

Table 24.0: A.3 Control

Code	Area	Consideration	Context	Definition
3.1	Controls	Compliance		Compliance considers the activities needed to validate and report on the effectiveness of implemented controls.
3.1.1	Controls	Compliance	Control Verification	The activities that support verification of control mechanisms.

3.1.2	Controls	Compliance	Test and Evaluation	The activities that support the test and evaluation of security capabilities and requirements.
3.1.3	Controls	Compliance	Reporting	The activities required to comply with security and privacy reporting requirements, performance metrics, associated costs and other information.
3.2	Controls	Control Categories		Control categories consider the specific activities, technical implementations and processes instituted to reduce or eliminate known vulnerabilities.
3.2.1	Controls	Control Categories	Management	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. See FIPS 200, ISO/IEC 27001, ETSI cyber security and ANSI/ISA 62443 etc
3.2.2	Controls	Control Categories	Operational	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people, as opposed to executed by systems. See FIPS 200, ISO/IEC 27001, ETSI cyber security and ANSI/ISA 62443 etc
3.2.3	Controls	Control Categories	Technical	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. See FIPS 200, ISO/IEC 27001, ETSI cyber security and ANSI/ISA 62443 etc

REFERENCE

S/NO	DOCUMENT NAME
1.	FEDERAL ENTERPRISE ARCHITECTURE FRAMEWORK VERSION 2
2.	TOGAF 9.2
3	ENTERPRISE ARCHITECTURE AS A STRATEGY, BUILDING FOUNDATION FOR EXECUTION BY JEANNE W.ROSS, PETER WEILL, DAVID C. ROBERTSON (MIT Sloan School's Center for Information System Research (CISR)

NOTE: The contents of this document are mainly derived from the above two frameworks and the book but customized to Nigerian environment.