Ghana Government Enterprise Architecture Framework

Version 2.0

TABLE OF CONTENTS

TABLES

FIGURES

ACRONYMS & ABBREVIATIONS

ACF	Architecture Content Framework
ADM	Architecture Development Model
CEAF	California Enterprise Architecture Framework
CIO	Chief Information Officer
CPM	Collaborative Planning Methodology
DLM	Dissemination Limiting Marker
EA / EAs	Enterprise Architecture / Enterprise Architects
EPA	Environmental Protection MDA
FEAF	Federal Enterprise Architecture Framework
GEAW	Government Enterprise Architecture Workgroup
GGEA	Ghana Government Enterprise Architecture
GAS	Ghana Audit Service
GCSA	Ghana Cyber Security Authority
GES	Ghana Education Service
GFS	Ghana Fire Service
GHS	Ghana Health Service
GIS	Ghana Immigration Service
GJS	Ghana Judicial Service
GMA	Ghana Meteorological MDA
GPS	Ghana Police Service
GPSC	Ghana Public Service Commission
GRA	Ghana Revenue Authority
ICT	Information & Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IRAP	Information Security Registered Assessors Programme
ISO	International Organization for Standardization
JDF	Job Description Form
MoD	Ministry of Defence
MoE	Ministry of Education
MoF	Ministry of Finance
MoH	Ministry of Health
MoI	Ministry of the Interior
MLG	Ministry of Local Government
NDPC	National Development Planning Commission
NITA	National Information Technology MDA
OHCS	Office of the Head of Civil Service
RA	Reference Architecture
SFIA	Skills Framework for the Information Age
SME	Subject Matter Experts
SOA	Service Oriented Architecture
TOGAF	The Open Group Architecture Framework

1 INTRODUCTION

The Government of Ghana (GoG) has embarked on an ambitious agenda to transform government operations and service delivery and is investing heavily in data centre infrastructure, systems, and networking capabilities to create an enabling environment for ICT-based business transformation. But to be successful, budgetary investments alone will not suffice.

We will also need to build human resources capacity and establish organizational structures and processes based on international best practice standards to govern ICT, deliver ICT services, manage information security, and prioritize ICT procurement government-wide.

> In our current "silo" based environment, there is little data sharing between MDAs, little attention to interoperability standards, and little visibility across GoG's ICT landscape, which makes effective planning impossible. This will all have to change - but creating the necessary organizational structures and processes is a complex task that requires careful planning, coordination and monitoring.

Just as any structure requires a well architected blueprint that defines and describes the materials for the structure, the way to build the structure, and the ultimate shape of it, organizational transformation requires a blueprint that describes the components of the organization, their relationships, and the way to achieve the mission and vision of the organization. Building or managing an organization without architecture is as inefficient as building a structure without a blueprint.

Enterprise Architecture (EA) defines the future state business processes, information, technologies, and organizational structure in a coordinated fashion, and provides strategies, standards, best practices, guidelines, and recommendations for all the components of an enterprise that play a role in or have an impact on achieving enterprise goals and objectives.

> The *Ghana Government Enterprise Architecture Version 2.0 (GGEA v.2.0),* as detailed in this document, and the companion *eGovernment Interoperability Framework (eGIF)* provides the blueprint and roadmap to build the GoG's future state. The GGEA v.2.0 is an enabler for business transformation and provides the guidelines needed to ensure that GoG moves efficiently and effectively towards fulfilling its strategies and objectives, and therefore towards its mission and vision.
>
> With consideration of and cross-referencing to GoG's articulated strategies and objectives (e.g., eGovernment Implementation Strategy, ICT4AD, MDA level strategies and service charters, NITA Strategic Plan, etc.,) the GGEA v.2.0 defines the future vision and direction for ICT use to support service delivery by GoG, and will enable and promote standardization and harmonization of ICT investments across government to ensure a better alignment of these investments with government business strategies and objectives. By doing so, the GGEA v.2.0 programme will result in improved management and quality of information, more efficient business and information technology operations, better return on existing investments, reduced risk for future investments, and a faster, simpler, and cheaper procurement process.

1.1 Background

Ghana's first GGEA and eGIF were drafted in 2007 and adopted in 2008. The original GGEA-eGIF were modelled on the U.S. Government's Federal Enterprise Architecture (FEA), which was the most developed framework at that time.

The first iteration of GGEA-eGIF covered all government services across all government entities ('Whole-of-Government' approach), and aimed to move the government towards standardized technology and rationalized data and applications. The output of the first iteration of the initiative was:

1. Target architecture for government service delivery
2. Technology standards and guidelines
3. Initiation of EA maturity programme
4. Governance and compliance framework to guide the above

In addition, the project also identified a set of projects to be implemented to achieve the target architecture. These projects ranged from simple enhancements to existing systems, through to major procurements of new infrastructure and shared applications. Most of these projects have since been implemented.

In practice however, the 2008 GGEA-eGIF faced significant implementation challenges which led to limited uptake and utilization, notably:

- Lack of a single centralised coordinating authority to manage the implementation of the GGEA.
- Lack of enforcement policies and guidelines on compliance with the eGIF.
- Lack of access to sufficient funding to educate MDA and NITA staff and promote the adoption of GGEA-eGIF.

Since then, there have been many disruptive IT innovations which have implications on the underlying technology and management approaches and hence there is a need to redesign the concepts of digital service delivery to respond to current technologies, IT management and governance, and the demands posed by global or regional emergencies such as the COVID-19 pandemic. For example, the existing GGEA either does not address, or insufficiently considers now common technologies such as cloud computing, Internet of Things, mobile money interoperability, Big Data, and Artificial Intelligence.

Moreover, the mandate of some MDAs has changed significantly, and many new institutions and regulatory frameworks have been introduced.

As such, the original GGEA-eGIF framework is no longer relevant, and needs significant revision and update to address these challenges and enable the Government of Ghana to effectively implement its e-Government strategic priorities and achieve digital transformation of government service delivery.

To address these issues, we are renewing our commitment to the development, implementation and ongoing maintenance of the Government of Ghana Enterprise Architecture and eGovernment Interoperability Framework. GGEA and eGIF v.2.0 embody that renewed commitment, providing updates to account for the evolution of technology since 2008, and putting in place a more comprehensive approach to organizational and human factors designed to strengthen implementation.

An updated GGEA-eGIF v.2.0 will help in managing the increasing complexity of GoG's burgeoning IT portfolio, supporting business and IT strategic planning and budget prioritization, delivering a road map for changes, supporting system development, etc., and address increasingly important issues such as legacy transformation, business changes, infrastructure renewal, and application systems renewal and business/IT alignment.

1.2 Business Case for the GGEA

In today's world, e-Government - for every country, developed or developing - is a necessity to achieve better governance, and the GoG has long committed to exploiting ICT to manage its information and internal processes more effectively to achieve greater efficiencies. This commitment is crucial to maintaining and improving service levels to the public, enabling sustainable government operations, and helping to build a strong, healthy, smart and fair economy.

Nonetheless, we remain under continuous pressure to improve to meet increasing service delivery expectations. Meeting the challenges of improving citizen services, adapting to changing Government requirements and legislative mandates, reducing the complexity of bureaucratic organisational structures and processes, and generally improving the business of Government will require more that just procurement of computers and applications.

The increasing demands we face require a technology driven transformation of the way MDAs operate - a new trajectory to improve service delivery and address expanding responsibilities for maintaining the social fabric and advancing social justice – all while fiscally constrained.

If MDAs are to meet the challenges of a modern digital economy, defining and effectively implementing an Enterprise Architecture framework is even more important now than it was in 2008, and grows more urgent year by year.

Adopting EA at a national level has proven to be a key enabler of e-government success because it provides an effective means of improving interoperability, reducing costs, and avoiding duplicated effort. Surveys show that nearly 90% of developed countries', and over 60% of all governments, have adopted and use EA frameworks to guide their e-Government efforts (Gartner). The United Nations' e-government rankings clearly show a positive correlation between e-government rank and having a national EA framework.

Enterprise Architecture is recognised as the most appropriate decision making and management framework for enabling MDAs to collaboratively provide seamless services and maximally leverage existing investments. At the highest level, EA is about organizing an enterprise's resources – its services, processes, information, applications, and technology infrastructure – and providing technical options and a supporting set of policies which help achieve desired business outcomes, technical standardization, and integration.

Research has conclusively demonstrated that EA offers the following benefits to government:

Process Effectiveness	**Opportunity Creation**
• Improved productivity • Increased business agility / reduced work-around	• Faster response to change and adaptation to new business requirements

• Lower costs • Faster cycle time • Improved output quality • Improved information quality • Improved citizen satisfaction	• Faster deployment times • Improved opportunity identification • Improved support for new channels and services • Improved partner linkages and relations
Operational Efficiency • Lower infrastructure costs • Reduced risk of intrusion, loss and downtime • Lower implementation and support costs • Procurement efficiencies • Higher reliability • Reduced training needs	**Development Efficiency** • Greater IT components reuse • Faster system development and integration • Simpler upgrades • Reduced technical risks • Improved security management • Reduced training needs

Table 1 - Proven Benefits of Enterprise Architecture to Government

This revised and updated GGEA v.2.0 will ensure alignment of ICT projects with national and MDA level strategies and bring our transformation goals within reach.

Explicit linkages between GoG's strategic objectives and the GGEA lie at the heart of this initiative, and address several key cross-MDA outcomes to modernise the public sector:

- Information sharing and collaboration - allowing data to flow between the public, service professionals, and public service MDAs.
- Seamless, one-stop-shop channels – helping MDAs to effectively manage high data flow volumes while creating simplified, seamless service access channels for constituents.
- Information security - providing secure, Internet-based solutions that protect MDAs' sensitive information.
- Self-service - enabling organisations to improve constituent satisfaction and lower overhead costs through the development of self-service capabilities that facilitate the efficient exchange of information.
- Management decision support - enabling MDAs to accurately track, manage, and forecast costs and funding, to ensure current projects are realised and to maximise performance.
- Process efficiencies – allowing users to send and receive transactions (such as payments) faster, better and cheaper.
- Shared infrastructure – ability to create shared application and infrastructure services to improve services and reduce costs.

GGEA v.2.0 provides a clearly articulated blueprint and a shared vocabulary for defining the current and target architectures,[1] as well as a transition plan and performance measurements for assessing progress towards the desired transformation, based on a tailored and localized framework that delivers a comprehensive set of processes, policies, guidelines and tools to guide how we organize ours resources to support service improvement.

[1] In the EA context, the as-is state is called the Current Architecture, and the desired future (to-be) state is often called the Target Architecture.

The GGEA v.2.0 Target Architecture defines the different architecture reference models, the principles and the transformation strategy for the implementation of the GGEA, to ensure that:

1. Business strategy and target capabilities are clearly linked in a cascading structure from national strategy down to departmental or MDA strategy.
2. Cross-organization collaboration and corresponding target cascading architecture will be the key driver ensuring successful delivery of national strategy objectives in the target state.
3. IT and Enterprise Architecture governance will be substantially improved to centralize oversight via an appropriate Governance, Risk and Compliance (GRC) model in order to comprehensively manage all initiatives.
4. Enabling legislation to support a comprehensively executed enterprise architecture transformation roadmap will be identified and enacted.
5. A clearly defined national data model based on a citizen centric approach will enable each MDA to leverage sharable services.

The GGEA will put at the disposal of government a federated architecture which acknowledges that Government operations are predicated on a single enterprise composed of autonomous MDAs . MDAs will be responsible for their own enterprise architectures yet will be able to leverage and contribute to whole of-Government architectures and investments through a single consistent framework, thereby supporting MDAs to:

- deliver services in a coordinated, cost effective and efficient manner;
- improve the integration and alignment of decision making across the whole-of-government;
- support coordinated decision making about strategic directions, policies and standards;
- use information and ICT to achieve their business objectives;
- guide the development, use, and management of information and ICT resources in a coordinated manner over time;
- position themselves for future needs.

As such, the business case for the Government of Ghana to implement an enhanced and adaptive EA Framework is clear, and even more compelling today than it was in 2008.

1.3 Document Contents

GGEA v.2.0 defines GoG's future state service delivery landscape, information, technologies, and organization in a coordinated fashion, and provides strategies, best practices, guidelines, and recommendations for all the components of an enterprise that play a role in or have an impact on achieving enterprise goals and objectives.

GGEA v.2.0 maintains consistency with the structure of the original GGEA, which was based on the U.S. Government's Federal Enterprise Architecture Framework (FEAF), while drawing upon The

Open Group Architecture Framework's Architecture Development Method (TOGAF ADM) for developing and maintaining the enterprise architecture through an iterative and cyclic process.

This document represents the core output of the first ADM cycle. Future iterations will expand in scope and depth as GoG staff gain capacity in utilising the framework. It is structured as follows:

Chapter 1 – Introduction describes the background and context of the EA effort, its aims and expected outcomes, and the business case for implementation of EA in the GoG.

Chapter 2 – GGEA v.2.0 Framework presents an overview of the components and content of the EA and the approach GoG uses to develop and maintain it, including the Elements of the architecture (Governance, Architecture Principles, Architecture Method, Tools, Standards, Use, Reporting and Audit), the six Domains of the architecture (Performance, Business, Services, Data, Technology and Security) and the actionable, minimum core set of Deliverables of the architecture (Future State Architecture, Current State Architecture, Enterprise Transformation Roadmap and the Architecture Artefact Repository).

Chapter 3 – Services and Intended Use describes the services that NITA and MDA level enterprise architects will provide to participating MDAs, and how MDAs can make use of these services to achieve organizational goals.

Chapter 4 – Architecture Governance introduces the approach that will be used to govern GGEA v.2.0 to ensure that it is sustained and yields the envisioned benefits, and places EA governance within the wider context of organizational governance.

Annex A - GGEA v.2.0 Architecture Reference Models presents the guidance and taxonomies that are used to provide standardized categorization of MDAs' architecture elements across various viewpoints, allowing architects within an MDA and across the public sector to communicate using a common language to support consistent analysis and reporting across MDA and whole-of-government EA functions. The reference models correspond with the EA domains described in Chapter 2 (Performance, Business, Services, Data, Technology and Security).

Annex B – GGEA v.2.0 Architecture Governance Framework details the organisational structures, processes and procedures that will be followed in maintaining, updating and ensuring compliance with the enterprise architecture.

Annex C - GoG Enterprise Architects Skill-Set Requirements defines the minimum required skillset necessary to ensure that GoG enterprise architects are equipped to deliver the services and responsibilities described in Chapter 3.

2 GGEA V.2.0 FRAMEWORK

To understand the GGEA v.2.0 Framework, illustrated in the Figure below, it is necessary to understand the components that make it up. None of these components add value by themselves - meaningful value is delivered to stakeholders only when they are used together to provide a complete solution.

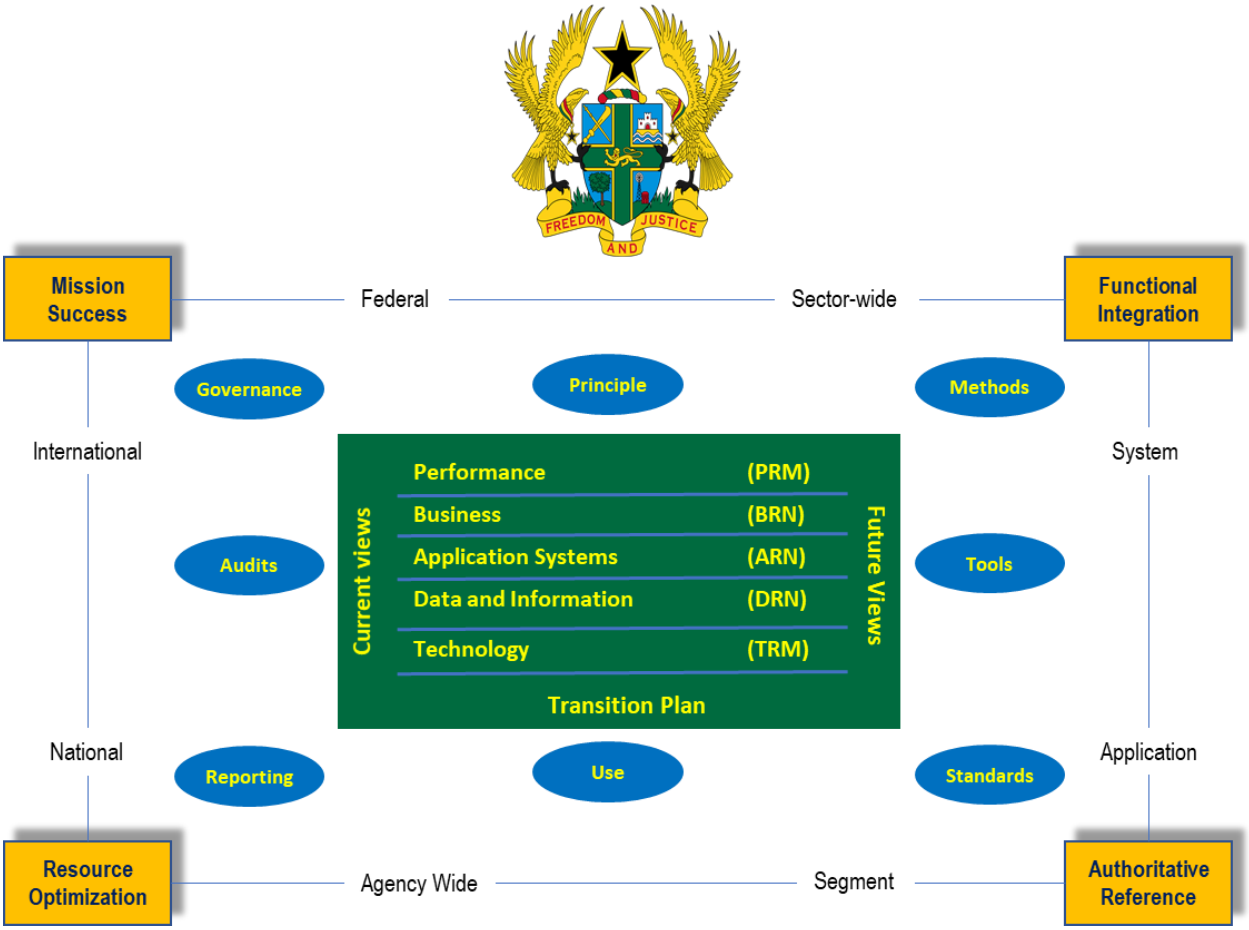

Figure 1 – GGEAF Overview

From the outside-in, GGEA has the following components:

- **Architecture Elements**: methods and processes that guide, support and govern the development of EA deliverables. GGEAF has eight elements: Governance, Principles, Methods, Tools, Standards, Use, Reporting, and Audits.

- **Architecture Domains**: allow MDAs to view themselves in terms of their strategic goals and the business services, processes, information, applications and the underlying technology that supports them. There are six domains within GGEAF; Performance, Business, Application Systems Data, Technology and Security.

- **EA Deliverables**: are outputs produced from the Architecture Domains. These are used by NITA and MDA executives in portfolio planning, decision-making and resource planning to achieve strategic business outcomes.

2.1 Architecture Elements

Element #1: Governance

Governance provides a means to manage additions and amendments to both the structure of the GGEA Framework and GGEA artefacts. The GGEA Framework, GGEA artefacts and accompanying eGIF are governed using the GGEA Governance Framework, as outlined below and described in detail in Chapter 4 – Architecture Governance, and Annex B – GGEA v.2.0 Governance Framework.

Architecture Review Board

An Architecture Review Board (ARB) serves the primary function of establishing, maintaining and enforcing Business and ICT architecture throughout an organisation.

The ARB is comprised of individuals who are experts in their field; typically, this will be the architect practitioners (across all architecture domains) as well as other technical and non-technical leaders from different areas of ICT.

The ARB acts as the approving and controlling authority for the following responsibilities;

- Establish, own and maintain the Organisation's EA Capability and its elements (principles, processes, resources, standards, guidelines, reference models, etc.).
- Monitor and enforce compliance of technical designs and components with the Enterprise Architecture – i.e., alignment of ICT investments and project designs to organisational goals.
- Achieving consistency between architecture domains.
- Maintaining and improving the maturity level of the architecture capability within the Organisation.
- Communicate the Organisation's EA blueprint throughout the organisation.
- Provide the criteria for decision-making in regards to architecture reviews and changes.
- Escalate decisions beyond the mandated authority to the appropriate (higher) body.

At a whole-of-government level under GGEA v.2.0, NITA will work with MDA leadership to identify and convene an ARB (EA Technical Working Group) that will have responsibility for the continued development and upkeep of the GGEA as well as assisting MDAs in complying with the requirements of the GGEA. At the MDA level, MDAs are encouraged to create their own ARB to manage the MDA's architecture in a way that best-fits the MDA, especially in terms of existing resource constraints.

Architecture Compliance

Architecture Compliance is a review of the compliance of a specific project against established architectural criteria (i.e., elements such as principles, standards, policies, etc.) and ultimately business objectives.

The review process involves identifying key roles, determining review scope, establishing or tailoring checklists of the review, executing the checklists (interviewing appropriate roles and assessing relevant documents), analyzing completed checklists and preparing the Architecture Compliance report.

> Architecture Compliance review will identify the level of conformance or relationship between the architecture model and the implementation of the product. The conformance levels are; Irrelevant, Consistent, Compliant, Conformant, Fully Compliant and Non-Conformant.

The Figure below illustrates the architecture conformance levels.

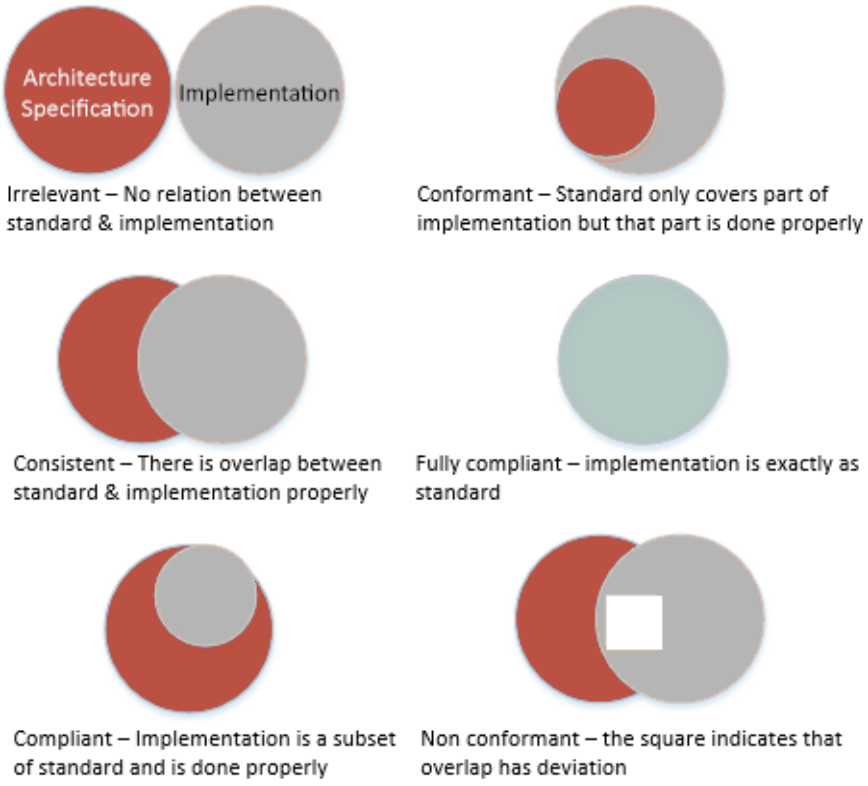

Figure 2 – Enterprise Architecture Conformance Levels

GGEA Governance Structure for MDAs

> Fully implementing an EA practice requires significant investments of time, effort and resources. MDAs should take pragmatic approach in developing their EA practice and move forward in a steady but measured way, within the available personnel and budgetary capabilities. Two examples of potential MDA EA governance structures are illustrated in the Figure below; for a

large MDA (left hand side of the diagram) and for small/medium MDA (right hand side of the diagrams). Most MDAs would be expected to fall on a continuum between these parameters, and choose from each structure as appropriate to MDA needs and capability.

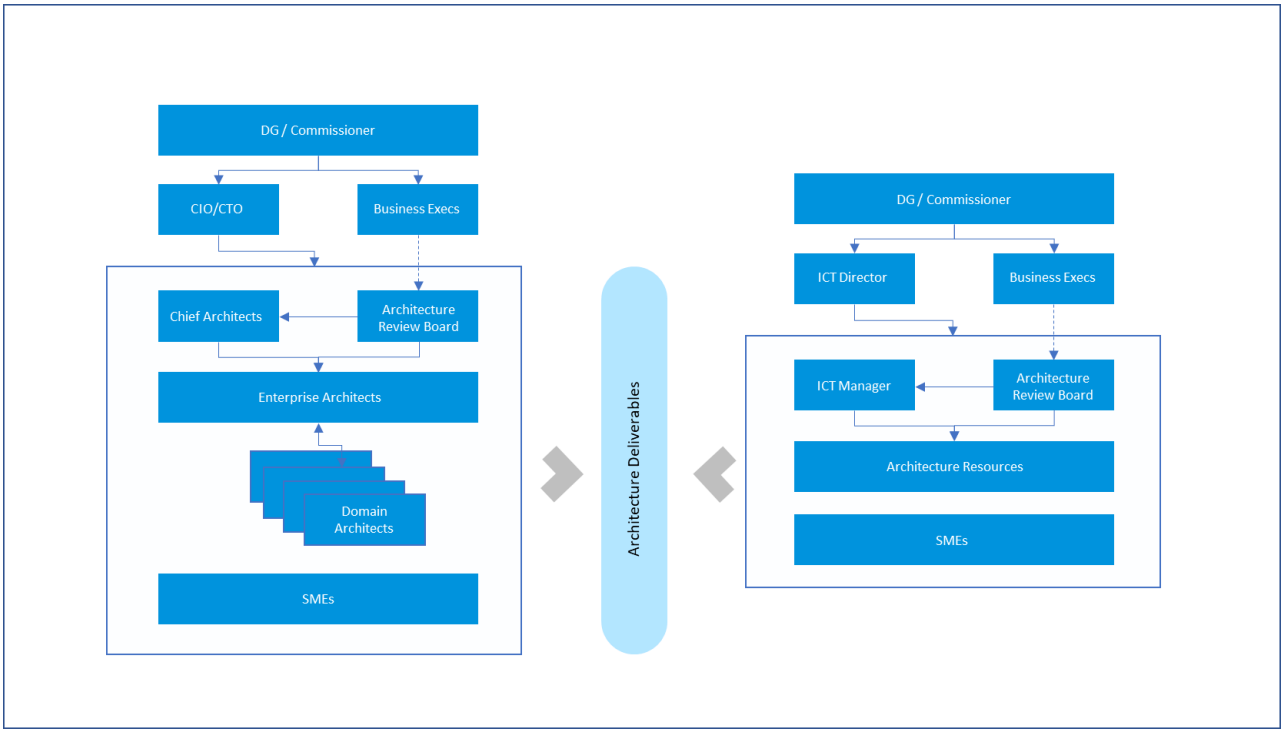

Figure 3 – Example of EA Governance Structure

Element #2: Architecture Principles

GGEA v.2.0 is underpinned by fifteen core Principles that guide EA decision making at both whole-of-government and MDA levels, to ensure consistency in the way business and ICT leaders consider options and make decisions.

A set of clear, strategic principles allows decisions to be delegated to the operational and project levels, by ensuring that decisions that comply with those principles align with the approved strategic direction and intent.

The GGEA v2.0 principles will support delegated ICT decision-making by:

- Providing clear, documented principles to guide staff in operational decisions that are in line with agreed strategic, MDA and project directions and outcomes.
- Providing specific direction for deciding between realistic and viable alternatives.
- Providing clear guidance in areas with the greatest potential to result in scope variation or misalignment with sector, MDA or project strategy.

- Aligning with MDA whole-of-government strategic principles, to support consistent sector-wide decision making.

- Undergoing regular review at key milestones to ensure consistency at all levels and to monitor compliance, use and understanding by relevant staff.

GGEA v.2.0 Principles

1. ***Align to deliver and leverage whole-of-government technology and service benefits.***

   MDAs must balance priorities between delivering whole-of-government benefits and MDA-specific benefits, and must actively collaborate to deliver solutions that provide benefits for many MDAs, rather than only for a few.

2. ***Comply with whole-of-government standards, methods and frameworks.***

   MDAs must comply with all policies, standards and frameworks approved and communicated under the GGEA. MDA ICT standards or frameworks must align with and support whole-of-government standards and frameworks.

3. ***Reinvest to drive digital transformation; invest to drive business sustainability.***

   A significant portion of any funds saved through ICT reform within an MDA should be retained and reinvested to fund digital transformation initiatives aligned to this Strategy, with sufficient ongoing funding to ensure sustainability.

4. ***Treat information as one of the State's most important assets.***

   Information is to be recognized and managed as an asset. All systems must ensure data is entered with integrity, stored and transmitted with appropriate security, and is easily accessible and discoverable to suitable search and analysis tools.

5. ***Design government services to be digital by default.***

   All systems and services must support easy access and use over the most appropriate and relevant digital channels.

6. ***Make decisions driven by business needs and informed by ICT capabilities.***

   ICT decisions must prioritise meeting business needs, while business decisions must prioritise practical ICT considerations. All significant MDA planning should include appropriate business and ICT representation and consultation in the process.

7. ***Source solutions using good PRACTICE.***

   The following prioritized sequence of options should be used when sourcing ICT solutions, stopping at the first option where sufficient business value can be realised:

Proof of concept – *using existing solutions, open source, freeware, pilot purchase, etc.*

Reuse – *an existing solution in government that delivers good enough value*

Adapt – *an existing solution that can be slightly modified to deliver good enough value*

Consume – *new "as-a-Service" offerings without significant ongoing commitment*

Test – *the available market, taking into account the next two requirements:*

Improve – *streamline business processes first before customizing a procured solution; and*

Commercial – *buy a commercially supported solution that delivers good enough value*

Engage – *suppliers to customize or develop a new solution.*

8. Actively seek to leverage expertise from professional, peer and social communities.

Projects must actively seek to identify and leverage skills and expertise available in internal and external peer communities to improve outcomes, reduce costs, or improve communication during the design, development, testing, implementation or use of new or improved services and systems. This can include online communities of practice, crowdsourcing, consulting with professional industry associations, etc.

9. Seek, develop and maintain appropriate internal expertise.

MDAs must attract and retain appropriate ICT expertise so that business decisions can be informed by suitably qualified, skilled, knowledgeable and experienced staff. MDAs should seek to access and leverage this expertise within the broader public sector before seeking external expertise.

10. Use human-centric design, and machine-centric automation.

All systems and processes must be designed to prioritise the user experience of the targeted user base. Human involvement in an ICT-enabled system or process should be targeted at decision and analysis points, with automation targeting the capture and exchange of data between machines or systems.

11. Keep things we control simple; coordinate complexity we don't control to interface simply.

ICT systems or processes under the direct management of government must be made as simple as possible through the elimination of duplication, removal of unnecessary redundancy, and the avoidance of unnecessary change complexity. Systems or processes that are not directly managed by government will have potential complexity to government minimised through the appropriate use of standards, controlled interfaces and managed gateways.

12. Seek solutions that are fit for purpose, not fit for everything.

ICT systems and processes must be designed or selected to meet the known purposes for which they are intended (which includes interoperability across the sector and compliance with

standards), and must not be designed to include, or selected due to, additional functionality or capabilities that are not required or desired within the immediate context.

13. If it can be shared, make it available to be shared.

All ICT resources, including staff expertise and underutilised assets, that can legitimately be shared for use by other MDAs or the public must be made easily discoverable and accessible.

14. Balance the consequential risks and benefits of all decisions.

The objective of ICT risk-benefit analysis must not be to reduce or minimise all risks, but to optimise the overall risk-benefit combination, in line with an MDA's reasonable risk appetite and tolerance.

15. Make decisions that are environmentally aware and socially responsible.

Project and operational ICT governance decisions must take into consideration any likely impact on the environment, community, or economy, with an objective of maximising benefits to the people of Ghana.

Element #3: Architecture Method

A mature EA practice seeks to translate the strategic vision of the organization into an effective enterprise transformation plan. It enables consistent planning across the organization and supports a risk-aware decision-making process to improve business outcomes through collaboration.

Enterprise Architects have an important role to play in the planning, implementation and performance measurement activities of identified investments/transformation projects. It is crucial that the EA methods are fully aligned and integrated with overall planning methods.

GGEA v.2.0 was developed utilizing a hybrid approach drawing from both FEAF and TOGAF, utilising the best of each approach for the needs of Ghana.[2]

Globally, the most widely used EA method in both private and public sectors is TOGAF's Architecture Development Method (ADM). The TOGAF ADM is a reliable, proven method for developing and managing the lifecycle of an

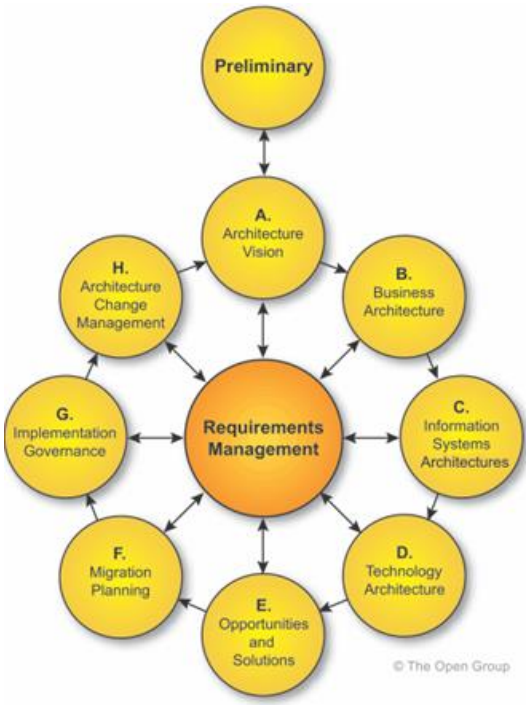

Figure 4 - TOGAF Architecture Development Method

[2] TOGAF – The Open Group Architecture Framework – is sponsored and supported by the Information Systems Audit and Control Association (ISACA). FEAF – the Federal Enterprise Architecture Framework, on which the initial 2008 version of GGEA was based, is owned and maintained by the U.S. Government.

Enterprise Architecture to meet the business and ICT needs of an organization. The Figure below illustrates the stages of TOGAF's ADM cycle.

The ADM is designed to be iterative over the whole process, between phases and within phases, and provides simple steps for developing an architecture which works well for non-technical stakeholders.

The ADM could be tailored to suit the needs of both MDAs and whole-of-government initiatives. For example, GGEA architecture domains can be mapped to phase B. Business Architecture, phase C. Information Systems Architectures and phase D Technology Architecture of the ADM process.

Another method that could be adopted for MDA or whole-of-government collaboration initiatives is FEAF's Collaborative Planning Methodology (CPM).[3] The CPM is a simple, repeatable process that consists of multidisciplinary analysis designed to support integrated planning, implementation and measurement activities. It is intended as a full planning and implementation lifecycle for use at all levels of scope (e.g., application, system, segment, MDA, sector, state, federal, and international).

The CPM is illustrated in the Figure below.

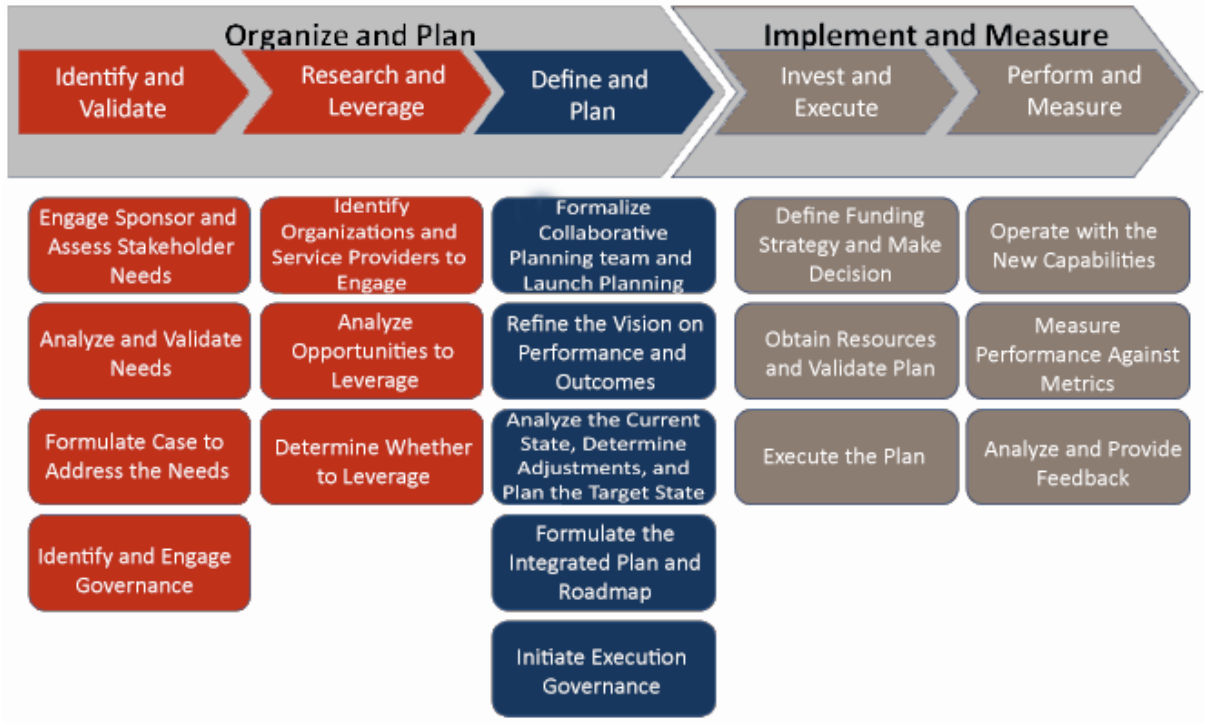

Figure 5 – FEAF Collaborative Planning Method

GGEA v2.0 does not prescribe a specific method at the MDA level. MDAs undertaking multi-MDA or whole-of-government initiatives should adopt the EA method that best fits the needs and maturity of their organization. TOGAF is probably a better framework for MDAs with less developed ICT

[3] FEAF – the Federal Enterprise Architecture Framework, on which the initial 2008 version of GGEA was based, is owned and maintained by the U.S. Government.

capabilities, and because it is the most widely used framework globally, there is an active online community from which to seek practitioner advice and support.

For development of future whole-of-government initiatives, it would make sense to adopt the method that is already being used by the majority of MDAs.

Element #4: Tools

NITA is currently undertaking a review of EA tools with the aim of selecting one that will meet all requirements of a whole-of-government EA Repository for GGEA v2.0. After review, the GGEA Working Group will draft a policy wherein MDAs who do not currently own or utilize a repository tool will be able to leverage the work being done by NITA to make use of a whole-of- government capability.

When choosing the EA repository tool, NITA will ensure that it it easy to access and use, supports integration with other existing EA tools and allows custom-built artefacts to be imported and stored.

Any repository used within the context of the whole-of-government EA should meet the required characteristics detailed below:

- Supports a Single Federated Repository across MDAs
- Supports multiple frameworks & modelling notation (TOGAF, ArchiMate, UML, BPMN etc.) interrelationships
- Supports EA artefact version control or rollback
- Able to generate editable architecture diagrams and show interrelationships within the repository
- Supports storage of non-model-based EA artefacts (i.e., office documents, images, PDFs, etc.) inside the repository
- Supports relationships between model-based EA artefacts and non-model-based EA artefacts
- Supports diagram import functionality and automated creation/mapping of architecture into the repository
- Supports import of data into the repository using MS Excel/CSV
- Supports user access control and permission on each of the following levels: Repository level, Folder level, Diagram level, Object level, Attribute level
- Able to reuse existing elements within the repository, such as: Folder templates, Diagram templates, Created Objects, Created Attributes
- Supports decision analysis capabilities, including at minimum gap analysis, impact analysis, scenario planning and system thinking
- Able to generate, save and export user defined reports and graphics in multiple documentation formats (i.e., PowerPoint, MS Excel, PDF, Image etc.)
- Supports EA artefact governance through the use of approval workflow
- Provides extensive strategy and IT portfolio management dashboard

Element #5: Standards

Standards are agreed ways of performing something such as managing a process or delivering a service, that are based on the collective knowledge of subject matter experts in the relevant fields and lessons learned from previous experiences. Standards are often voluntary; they serve as a reliable guide in approaching common problems in a consistent and efficient manner.

In EA, standards are essential to achieving interoperability, and increasing consistency and efficiency in terms of resource optimization through proven common methods and a shared language for analysis, design, documentation and reporting. EA standards typically contain sufficient level of detail built on repeatable patterns to encourage consistent and predictable outcomes, yet are agnostic and vendor neutral to facilitate reuse, replication and implementation. Without standards, EA deliverables will not be developed in a consistent manner and a like-to-like comparison will not be possible between applications, systems, services, lines of business and organizations.

GGEA v.2.0 incorporates applicable standards from leading bodies including the International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE) and the U.S. National Institute of Standards and Technology (NIST). In addition to these proprietary standards, GGEA v.2.0 also includes other bespoke standards developed specifically for the GoG context such as the domain Reference Architectures contained in Appendix A – GGEA Reference Models.

Element #6: Use

> The value of EA is in both the process and the products. Doing an architecture project provides a focus on a mission or support area of the organization, and the resulting analysis and design activities, if done correctly, support improvements in that area. Only an enterprise-wide architecture can provide an integrated view of strategic, business, and technology domains across all lines of business, services, and systems – which is key to optimizing mission capabilities and resource utilization.

At present, there is no other management best practice, other than EA, that can serve as a context for enterprise-wide planning and decision making. When an EA is viewed as authoritative by MDA leadership, then it becomes a catalyst for consistent methods of analysis and design, which are needed for the organization to remain agile and effective with limited resources. Section 3, following, details GGEA intended usage and services within MDAs.

Element #7: Reporting

As with any other programme/initiative/project, MDAs need to be able to report on the EA function's activities and measure the benefits to maintain visibility of current organizational capabilities and

future opportunities. EA reporting is about assembling and presenting relevant metrics in a manner that is meaningful for the intended stakeholders.

For this purpose, architecture artefacts that are created, collected and stored in an EA repository system need to be easily accessible by, and published to, relevant stakeholders. These artefacts support the creation of various EA reports in a standardized way using established metrics and a documented method.

> At the end of each financial year, MDAs will be asked to report their self-assessed alignment with the GGEA to executive leadership and decision makers so that management challenges identified by the EA function can be addressed, either by commitment of additional resources or through changes / improvement to the EA function itself.

Under GGEA v2.0, the following reports will be produced at the MDA and whole-of-government levels:

- Annual EA Plan, including detail on EA function current status and progress to date, and overall EA segment by segment development planning
- Enterprise Roadmap
- ICT / Business Strategic Alignment
- Application Portfolio Rationalisation Results
- EA Maturity Scorecard
- Business Process Maturity Scorecard
- Catalogue of Reusable Services and Assets
- Reference Architecture Technology Standard Matrix

Element #8: Audit

> EA as a practice focuses on the alignment of business strategy and IT capability. EA defines the current-state and target-state architectures in line with government-wide IT assets and capabilities, business strategy, and strategic priorities, and guides the process of planning and designing IT capabilities to meet the desired objectives of the organization.

To underpin the EA practice, audits are conducted as part of a process that involves identifying key roles, determining audit scope, establishing or tailoring checklists of the audit, executing the checklists (interviewing appropriate roles and assessing relevant documents), analysing completed checklists and preparing Audit report.

Under GGEA v2.0, the primary objectives of the audit will be to determine the:

- Extent to which MDAs have developed and documented an “as-is” and “to-be” EA and migration strategy, and complied with GGEA v2.0 guidelines and requirements;
- Maturity level of the MDA’s EA management processes using the GGEA guidelines; and
- Effectiveness of the MDA’s management controls and processes to manage its EA efforts.

2.2 Architecture Domains

An architecture domain is an abstract view of an MDA, or the government as a whole, that provides stakeholders with the ability to see the organization through different lenses. Depending on the lens being used, it allows for specific analysis and modelling tasks to be undertaken at the required depth to provide clarity on how an organizational component is used to support the goals of the organization.

For this purpose, GGEA v2.0 adopts the following six architecture domains: Performance, Business, Application Systems, Data, Technical and Security.

The Performance Domain - is focused on designing and implementing effective business measurement systems and performance architectures. It identifies measurement needs and describes the types of measurement that can support identified needs and define effective measurement indicators.

The Business Domain - provides a taxonomy for classifying a functional (as opposed to an organizational) view of Lines of Business (LoB). It articulates the capabilities required for achieving the desired performance outcomes and business objectives and links the capability through to the supporting business processes.

The Services Domain - serves to identify and classify horizontal and vertical application system service components that support MDAs and their ICT investments and assets. Application architecture encapsulates business services, applications, application capabilities and components.

The Data Domain - serves to identify and classify data assets, and supports information sharing and reuse across the public sector. It promotes uniform data management practices by enabling MDAs to agree, establish and support a common language and standards for information sharing.

The Technical Domain - is a component-driven, technical framework categorizing the standards and technologies used to support and enable the delivery of business functions and services.

The Security Domain – provides building blocks to build layered security mechanisms within a service, allowing multiple preventive and detective controls to be integrated as part of risk mitigation strategy. The criteria for risk acceptance will be based on the security classification of information assets used in the delivery of the service.

Each domain can impact or influence the others. For example, the Business domain drives what the Services are, but at the same time, the Business is dependent on the Services to operate and achieve its goals.

Detailed architecture reference models for each of these domains are contained in Annex A.

2.3 Architecture Deliverables

GGEA v.2.0 is designed to operationalize and expand the focus of MDA and cross-MDA EA functions, thereby creating actionable EA deliverables. Actionable in the sense that the architecture analysis, artefacts and documentation can be used by executives, managers, and staff to support and improve portfolio planning, resource planning and decision-making. Actionable deliverables have a direct relationship to strategic goals and business requirements, and they drive change towards the desired future state.

GGEA v.2.0 identifies the following actionable deliverables as the minimum set of core artefacts:

1. **Future State Architecture**
   A view that represents the target state architecture of an MDA or the government as a whole, within the context of its strategic goals and its operating model.

2. **Current State Architecture**
   A view that represents the current state (baseline) architecture of an MDA or the government as a whole. An organisation cannot start a transformation process without knowing its starting point.

3. **Enterprise Transformation Roadmap**
   A guide that contains a necessary set of actions to transform the MDA or government as a whole from its current state architecture to its target state architecture.

The Figure below illustrates the recommended minimum set of EA deliverables.

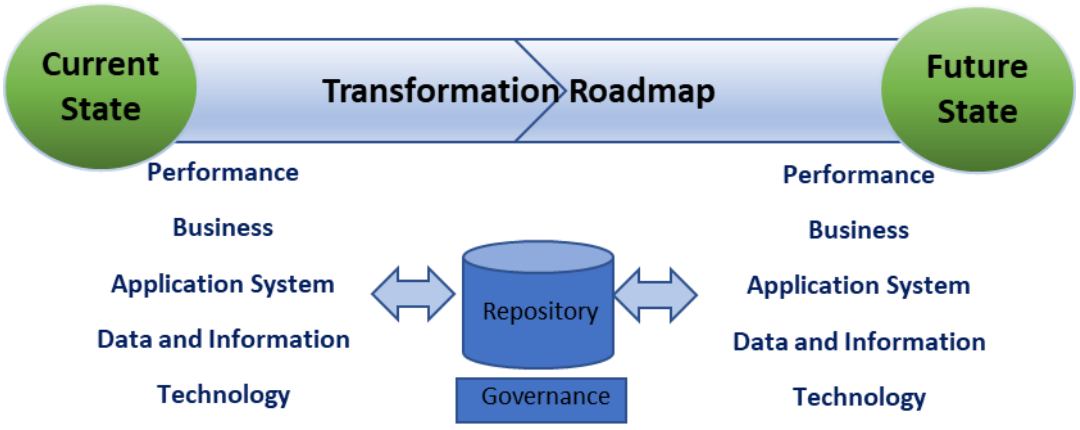

Figure 6 – Minimum GGEA v.2.0 Deliverables.

The Current State Architecture and Future State Architecture can be thought of as two views of the same organization at different points in time. They take the form of a set of interconnected models that support better planning, decision-making and management within both MDA and whole-of-government strategic initiatives. These models describe the relationship between an organization's

strategic goals, business functions, information, and enabling applications and technologies in an explicit and manageable way.

The Enterprise Architecture Roadmap details the programmes, projects and initiatives planned to transition the organisation to the future state architecture (bridge the gap) in all five architecture domains.

For many MDAs, it will also be common to include one (or more) Transition State Architectures as additional deliverable(s) to show an architecturally significant state between the Current and Future State Architectures. A Transition State Architecture view is used to describe significant milestones towards the effective realization of the Future State Architecture.

Since public sector operations and strategic goals are not static, these deliverables must be updated and communicated periodically to reflect new realities (i.e., new current state) and changing directions (i.e., new target state).

The following sections describe these deliverables and a framework for an organized structure of the current and future state architectures of GoG organizations. It does not at this stage contain actual architecture views of particular MDAs or indeed the whole of government – as these can only be delivered when the GGEAF has been successfully implemented by an MDA / NITA EA functional unit.

2.3.1 Future State Architecture Views

The Future State Architecture views represent possible target states of the MDA / Whole of Government within the context of its strategic direction and operating model.

It defines the architecture required to meet MDA or whole-of-government initiatives. It describes what the architecture should look like, and will typically consist of the following models:

- **Future Performance Architecture** – describes the future state outcome-focused measurements of all other architecture domains.
- **Future Business Architecture** – describes the future state business capabilities and the business process model.
- **Future Services Architecture** – describes what business services, applications, and systems are necessary and relevant to the organisation and how those multiple applications work together to support the future state business process model and manage the information.
- **Future Data Architecture** – describes the structure of the organization's logical and physical data assets and the data management resources required to support the future state business process model.
- **Future Security Architecture** – describes the building blocks to build layered security mechanisms within a service, allowing multiple preventive and detective controls to be integrated as part of risk mitigation strategy.
- **Future Technology Architecture** – describes what logical software and infrastructure capabilities the organisation will require to support the future state business process model, information, and application services.

Future State Architecture views will also identify the motivational elements pertaining to the future state and relate them to the other architecture elements as described in Chapter 2.1 ***Elements***. As such, creation of Future State Architectures should take into consideration both MDA and whole-of-government vision and strategies.

> Creating the Future State Architecture first - before defining the Current State Architecture view - is considered best practice because it provides greater freedom in considering future possibilities, allowing architects to think about the business strategy and its requirements and how EA can best support them without being constrained by the limitations of the current environment. Doing Future State Architecture first will also assist in determining the level of detail necessary for the Current State Architecture to be meaningful.

One of the first activities in establishing an MDA level Future State Architecture view is to create diagrams and models that show how the organization should look, without redundant applications or systems and unnecessary processes. It also involves designing or using whole- of-government capability / reusable components that an MDA can leverage throughout the public sector.

> The type and depth of documentation of the models mentioned in the previous paragraph will be guided by the need for detail (using a 'just enough' approach) and answers to questions about objectives, requirements, applicable standards, time frames, and resources. To ensure interoperability and shareability of services, Future State Architecture views need to sufficiently describe the architecture components in each domain and specify their key attributes at a level of detail necessary to provide an authoritative reference and to communicate the benefits of the Future State Architecture to all stakeholders.

Additionally, models should incorporate whole-of-government GGEA v.2.0 Enterprise Architecture standards including the reference architectures as applicable, based on the required business capabilities. Reference architectures are a key input into creating future state architectures and generally will have broad applicability to most, if not all, MDAs.

Development of Future State Architecture covering all Lines of Business and architecture segments of an MDA could take a significant amount of time and resources to complete. Initially, this effort should focus on a small number of key business outcomes and the underlying segments to provide quick value and gain executive support. Note that narrowing down the focus of Future State Architecture can also be facilitated through developing the current state and gap analysis, fitness and strategic alignments of systems, etc. This incremental approach would allow an MDA's EA function to evolve over a period of time.

2.3.2 Current State Architecture Views

The Current State Architecture views represent the current state or baseline for the organization. It documents the current elements of the organization and for most MDAs will consist of the following models:

- **Current Performance Architecture** – describes the existing state of outcome-focused measurements, if any, across all other architecture domains.
- **Current Business Architecture** – describes the current state business capabilities and the business process model.
- **Current Services Architecture** – describes what business services, applications and systems are currently in place to manage the information and support the business processes including their key components and interactions.
- **Current Data Architecture** – describes the structure and content of an organisation's existing digital and physical data assets.
- **Current Security Architecture** – describes current measures in place to protect GoG's ICT systems and information.
- **Current Technology Architecture** – describes what software and infrastructure is being used to support the organisation.

It is important in establishing a current state architecture view to create diagrams and models to show current operations and interactions between data, function and platform components in the context of the five architecture domains. Additionally, Current State Architecture views also represent the motivational elements pertaining to the current state as (identified) assessments, requirements, and constraints across all architecture domains.

The type and depth of documentation of the models should be guided by the need for detail (again, a 'just enough' approach), making sure that the focus remains on business outcomes and is not diverted to documentation for its own sake.

Apart from providing an initial baseline in the development of an Enterprise Roadmap to the future states, the Current State Architecture assists in identifying dysfunctions, duplications, complexity and dependency of existing solutions, and facilitates continual updating of infrastructure documentation.

The importance of getting an accurate picture of an MDA's current state cannot be overstated because it is fundamental to producing a quality and actionable roadmap– in other words, we need to know where we are to devise a reliable plan to get to where we want to be.

2.3.3 Transformation Roadmap

The Transformation Roadmap provides a guide on how to transition from the current state architecture to the future state architecture through a prioritized sequence of interdependent transformation programmes, projects and other initiatives. It promotes a strategic, long-term (GGEA v.2.0 will use a 5-year cycle) focus on business outcomes and, with an appropriate governance process in place, facilitates continuity in the delivery of business capabilities (e.g., avoids loss of direction when key business or ICT leaders change). It puts high-level strategic change into perspective and focuses on capturing and communicating the big picture.

A well-designed Transformation Roadmap also specifies key business outcomes expected from each programme/project/initiative; when a specific business outcome will be achieved, when a specific

business and/or information technology objective will be accomplished and how those outcomes and accomplishments will be measured. Without such measurable objectives, it may not be possible to validate the value and progression of programmes and projects (during their execution) towards the target Enterprise Architecture and in turn this can affect the governance of those programmes and projects.

Both the Future State Architecture and the Transformation Roadmap can be incrementally developed through lines of business, segments or domains by focusing on a few key business outcomes for each increment.

The Figure below illustrates the recommended GGEA v.2.0 approach to producing a sensible, achievable and defensible Enterprise Transformation Roadmap.

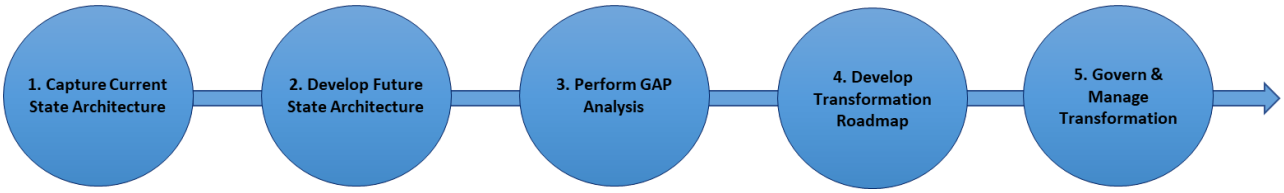

Figure 7 –Recommended Approach in Building Enterprise Transformation Roadmap

The steps in Figure 7 above are described in more detail below:

1. Develop desired future state architecture.

2. Develop an understanding of current state architecture.

3. Perform gap analysis between future and current state architecture views.
   The outcome of the gap analysis is to identify required business and technology transformation initiatives to close the gaps. These transformation initiatives are the core of the Transformation Roadmap.

4. Describe and prioritise all initiatives identified during the gap analysis.
   It is critical that MDAs involve, engage and consult all relevant stakeholders throughout this step. Each initiative should be described (typically in one or two pages) with key information such as; why the initiative is needed, drivers, business impact and expected outcomes, organisational priority, stakeholders, dependencies and estimated duration, cost and resources.

5. Define the optimal order in which all identified activities can be completed.
   Based on the information gathered for each initiative (dependencies, drivers, priorities, etc.) and consideration of the MDA's strategic outcomes.

6. Develop the Enterprise Architecture Roadmap.
   Capture and articulate the Enterprise Roadmap. Once produced, it needs to be published and communicated in a simple yet compelling manner for the intended audiences.

The Enterprise Roadmap is a key input to the following activities:

- Investment Management Review
  Provides information to support the investment review decision process from a government-wide perspective rather than in silos and thus prevents/reduces isolated/silo investments without whole-of-government perspective.

- Sourcing Practices
  Ensures there is alignment between Enterprise Architecture and other transformational processes being carried out in the GoG. Sourcing does not necessarily mean procurement activities; sourcing could mean the reuse or redeployment of existing public sector resources. However, if a gap is identified, then a procurement activity may be required.

- Whole-of-Government Initiatives
  Provides information to support identification of opportunities and planning for whole-of-government / multi-MDA initiatives by promoting the interoperability and shareability of systems and services.

- Programme/Project Governance
  Provides information to plan, execute, monitor and control programmes/projects to ensure incremental progress towards business outcomes, and business and ICT objectives. This, in turn, will contribute to the successful execution of multi-year programmes/projects.

The Figure below depicts an example of an EA Transformation Roadmap.

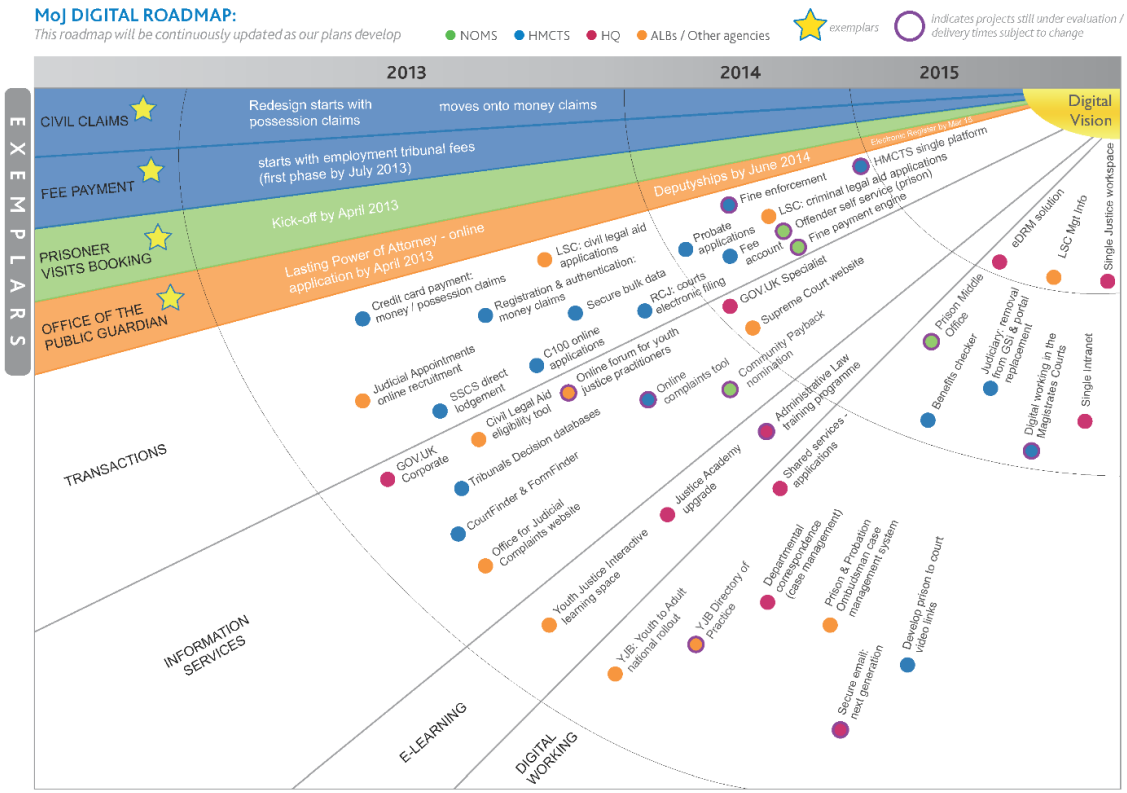

Figure 8 – Sample EA Transformation Roadmap

2.3.4 Architecture Repository

The final, minimal EA Deliverable is an Enterprise Architecture Repository, which is needed to support planning and decision-making using EA information/artefacts.

The EA repository is used to store, reference (link to), manage and access architecture artefacts created by the EA function. The repository can be as simple as a logically structured hierarchy of folders and files using typical desktop tools, or implemented with an EA tool that can make it easier to manage, maintain and publish EA products. The EA repository is a knowledge base that should be accessible by all relevant stakeholders and support EA governance processes.

MDAs who have already invested in their repositories should continue utilizing and gaining benefit from it. To ensure consistency between the whole-of-government and MDA repositories, MDAs will be asked to periodically review their repository for compatibility with the whole-of-government repository as appropriate.

3 GGEA SERVICES AND INTENDED USE

MDAs need to make informed strategic decisions because decisions made without the necessary and relevant information deliver suboptimal outcomes. The most common problems are that business units develop siloed solutions with increasing, unsustainable support costs, causing MDAs to abandon an integrated, cost effective and government-wide approach. A lot of unnecessary work may take place before the results of an uninformed or misinformed strategic decision finally surface.

GGEA v.2.0, through its services, will support a common understanding of needs across different areas of the government and facilitate collaboration in the planning of solutions to address specific business needs with a holistic view, rather than simply from a technology planning perspective. EA plays a pivotal role in ensuring the alignment of solution investments to the Government's strategic goals.

A mature EA practice seeks to translate the strategic vision of an MDA into an effective enterprise transformation plan. It will ensure decisions are made with full understanding of the strategic objectives and their implications for the MDA and across the public sector. It will also ensure decision makers have a clear understanding of cost, risk and benefits associated with each decision to assist them in finding the optimal solution.

What follows is a list of eight services, minimum, that the EA function within an MDA should provide to support an effective whole-of-government GGEA v2.0 EA function. The eight EA services include:

1. Assist with Business Strategy and ICT Strategy.
2. Application portfolio rationalisation.
3. Enterprise Architecture planning and actionable Enterprise Roadmap development.
4. Project prioritisation advice to help drive the business forward and improve programme outcomes.
5. Business and ICT initiatives development.
6. Standards establishment and architecture governance.
7. Solution architecture guidance and oversight.
8. Architecture patterns and reusability.

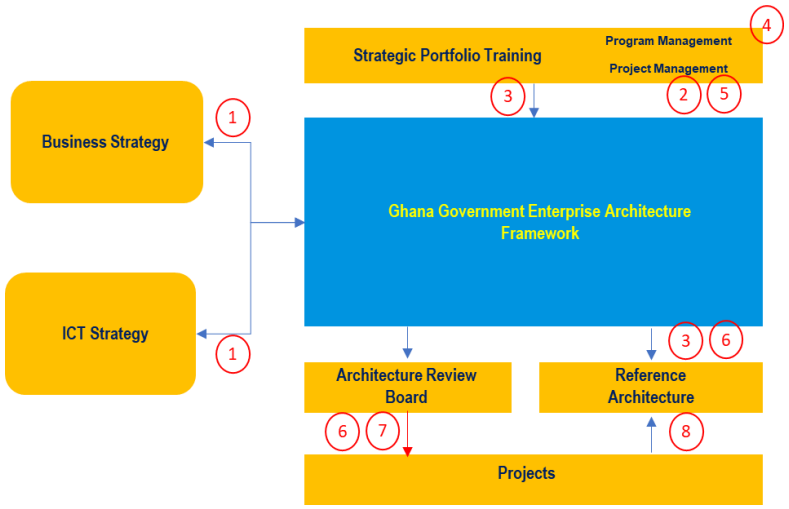

Figure 9 -GGEA v.2.0 service context

The Figure above illustrates the context of the EA services.

In order to develop a level of effectiveness of EA capability across the whole-of-government, it is envisaged that MDAs will charter their EA teams to provide these services, as described in detail below.

3.1 Assist with Business Strategy and ICT Strategy

A Business Strategy can be defined as a set of guiding directions/principles that when adopted by the MDA, provides the mechanism to generate desired decision-making. It sets the strategic direction and what needs to be done to achieve/accomplish key objectives. It should also include a clear and focused roadmap that guides the prioritization of initiatives. Typically, a business strategy spans across a number of years (e.g., 5 to 10 years).

An ICT Strategy is focused on how technology will enable the business to achieve its strategic goals. It specifies the contribution required by ICT to support and deliver strategic business outcomes successfully. The ICT strategy primarily focuses on the applications, data and technologies required to deliver business services, along with the people or organizations who directly interact with (or manage) them.

To deliver value, the ICT strategy needs to be aligned with the business strategy. ICT investment must be made in a way that it demonstrates support for the achievement of business strategic goals. The development of the aspirational and achievable business strategies depends on a good understanding of the capabilities of the existing and available ICT services that can enable them.

EA aims to clearly show how ICT investments are linked to strategic goals and how these investments will help achieve measurable business outcomes. It is because of this strategic perspective and future thinking that the EA role is well suited to assist in the development of Business and ICT strategies.

Figure 11 below describes the role of GGEA v2.0 in assisting with the alignment of ICT Strategy with Business Strategy.

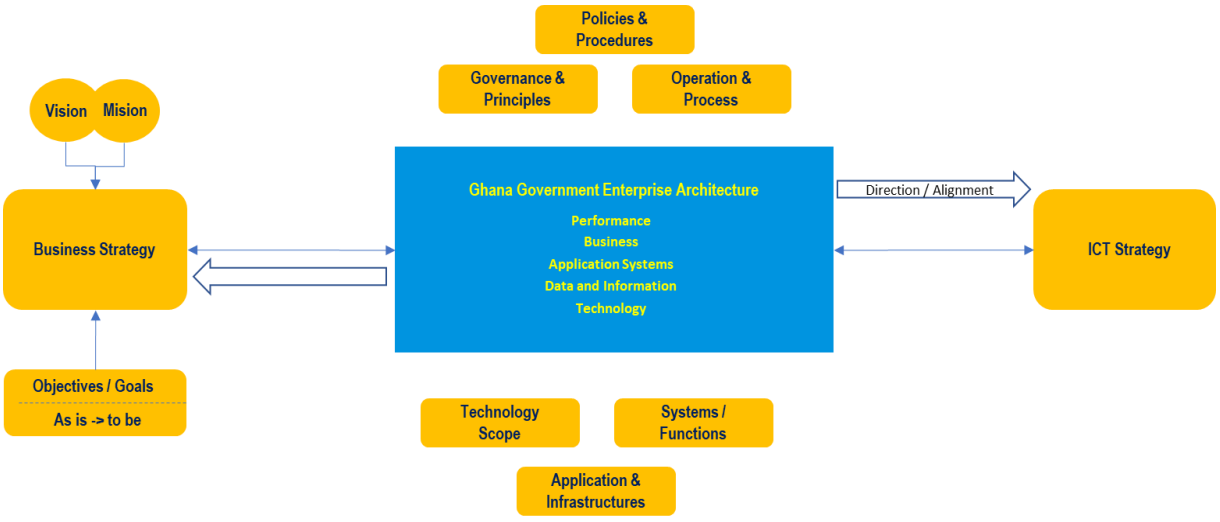

Figure 10 – GGEA v2.0 Role in the Context of Business and ICT Strategies

To assist with the development of business and ICT strategies, GGEA v2.0 will provide:

- An understanding of how emerging and innovative ICT solutions can drive business efficiencies.
- Shaping of strategic vision and goals to ensure they are achievable and viable with the technology available now and into the future.
- An understanding of the synergies available from the strategic paths of different business units within the MDA, and similar industry segments outside the MDA and across the whole-of-government.
- Understanding of what existing ICT capabilities are available, assessing their business and ICT fitness and identifying capabilities that can be reused or leveraged to support the strategic vision.
- Facilitation of the alignment of ICT strategy with business strategy.

3.2 Application Portfolio Rationalization

"Application rationalization often occurs after an IT organization accumulates an unmanaged collection of applications through shifting business strategies or mergers and acquisitions. The clean-up can include replacing, retiring, modernizing or consolidating applications." Gartner[4].

Based on the above definition, application rationalization is part of an Application Strategy that looks at whether an organisation needs to replace, retire, remediate or consolidate legacy applications. As part of this exercise, the organisation should assess whether the chosen 'clean-up' decision assists in streamlining existing business processes, to increase overall efficiency, reduce complexity, free up a budget for more business-critical initiatives and ensure that ongoing costs and resources are value for money.

Figure 12 below shows an overview of the application rationalisation processes.

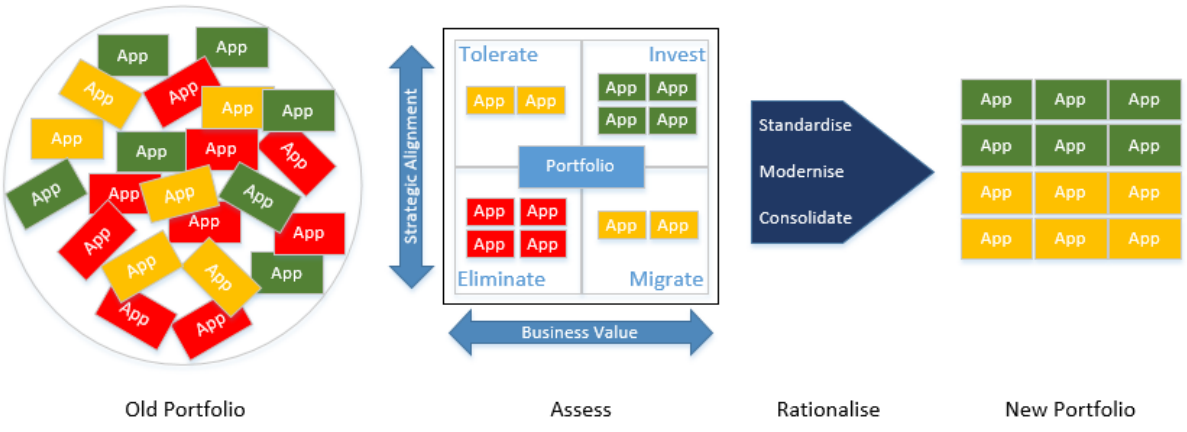

Figure 11 – Portfolio Rationalization Overview (Gartner, July 2013)

[4] Taken from Gartner's Application Rationalisation Key Initiative Overview (ID: G00252063, published: 25 July 2013, refreshed: 11 February 2015), more information on this link: http://bit.ly/WEAF-link7.

Significant savings can potentially be made through a sound understanding and management of an MDA's application portfolio. EA can assist the MDA in developing a well maintained and appropriately structured application portfolio strategy; MDAs will have the ability to identify duplication of application functionality across the MDA technology landscape.

Application rationalization plans can be developed and built into future planning as applications reach end-of-life or as ICT and business plans evolve.

To support the applications rationalization exercise, GGEA v.2.0 can assist in guiding how MDAs initiate and implement the following activities:

- Retiring applications with low business value and low level of strategic alignment.
- Modernising applications with high business value and low level of strategic alignment.
- Consolidating or reprioritising applications with low business value and high level of strategic alignment.
- Eliminating applications that are identified as being redundant or duplicate.
- Standardising common technology/infrastructure platforms.

Figure 13 below shows how the mapping of applications in relation to their business value and their strategic alignment can assist with rationalizing the application portfolio, using Gartner's TIME (Tolerate, Invest, Migrate and Eliminate) analysis.[5]

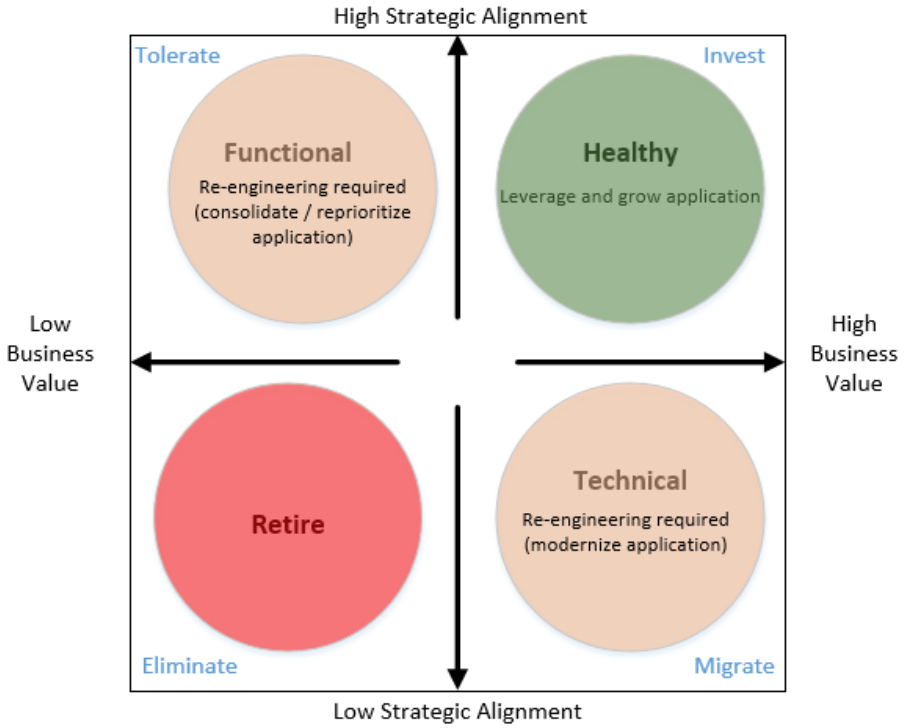

Figure 12– Mapping of Applications Using Gartner's TIME Analysis

[5] Based on Gartner's Application Portfolio Triage: TIME for APM (ID: G00169227), published on 5 August 2009), more information available at this link: http://bit.ly/WEAF-link12.

MDAs should understand their strategic initiatives, potential and planned projects to prevent new initiatives delivering duplicate solutions. It is imperative that what already exists is defined within the MDA and what is required to support other future initiatives (current vs. future state). GGEA v2.0 will provide the underlying data necessary to make informed choices, enabling MDAs to reduce costs and minimize system complexity.

3.3 Enterprise Architecture Planning and Actionable Enterprise Roadmap Development

An effective EA practice provides the skills and methods needed to translate business and ICT strategy into an achievable and actionable roadmap, helping lead an organisation through business transition.

Transitioning an organisation to meet a significant change agenda requires a big picture approach to ensure all impacts, opportunities and constraints are well understood and considered. It requires an understanding of the business' desired future state and how to best transition towards it, in a manner that ensures risk is appropriately managed while maintaining minimal disruption to business activities throughout the process.

Taking an organisation-wide perspective ensures that all interrelationships and interdependencies are understood and built into a roadmap that seeks to deliver both tangible business benefits continuously and progressively, and to sequence technical dependencies to minimise future work effort.

GGEA v2.0 will provide both tools and guidelines for Enterprise Roadmap development, as described in Section 2.3.3.

3.4 Project Prioritization Advice to Help Driving Business Forward and Improve Programme Outcomes

Enterprise Architects' (EAs) understanding of Business and ICT strategies and priorities combined with their understanding of how to best sequence and group ICT activities enable them to provide well-considered advice on project prioritization. Project prioritization helps to drive business forward efficiently which in turn improves overall business outcomes.

EAs understand what activities are required to transition a programme of work that needs to be broken up into projects, including:

- Grouping activities that deliver discrete pieces that are immediately useful and valuable to the business with the minimum amount of effort.
- Grouping change to minimise business disruption by avoiding multiple instances of business process change.
- Grouping closely related technology change together.
- Grouping activities that will deliver key foundation ICT pieces.

Utilizing the GGEA v2.0 Framework, project prioritization and sequencing will be driven by a reconciliation of:

- Business priorities and progressive delivery of items that provide business value.

- Project complexities and Interdependencies through ICT components, business components and their interdependence on separate business activities.
- ICT constraints and cost avoidance from items such as license agreement renewals, end of vendor supports, etc.
- Risk value of the project vs projected organisational benefit.
- Alignment of the project to the approved MDA's future state architecture.

3.5 Business and ICT Initiatives Development

To get project approval, an MDA typically requires a clear description of the project concept and its business case to justify the undertaking of the project. The business case also documents the requirements, the desired benefits as well as common agreements on how the outcomes will be measured.

GGEA v2.0 EAs will be uniquely positioned to assist business and technology leaders with the development of project concept and business case documents. EAs can proactively assist by providing the following capabilities:

- Brings the experience to understand how the big pieces of the solution can be assembled to meet the objectives of the business case and assist the development of cost estimates for solution options.
- Brings a thorough knowledge of an MDA's ICT landscape to recognise what can be reused, leveraged or interfaced to, what pieces of other projects will deliver and what is planned for the future. All of these bring opportunities or constraints to the business case.
- Through a knowledge of emerging technologies, an EA understands what can be leveraged to provide solution options.
- Brings a knowledge of the business and ICT strategies to ensure the proposal will be fit for purpose and can deliver the required strategic benefits.

3.6 Standards Establishment and Architecture Governance

EAs are skilled in establishing standards, guidelines and principles that guide ICT systems development including the establishment of appropriate governance and assurance processes to manage how they are applied.

Standards and principles guide the development of solutions in a systematic way leading to predictable outcomes that are the key to successful delivery of projects. Governance processes ensure the agreed approach is followed and any exceptions are considered at the appropriate level of decision-making.

Exceptions to the standards are at times necessary to exploit new opportunities or to avoid constraints. An EA role is best positioned to understand if the benefits of the exception will outweigh the introduction of non-standard aspects into the environment.

Ideally, standards, guidelines and principles should be highly accessible to projects from a single location and managed in a controlled way. The Architecture Repository established under GGEA

v.2.0 will make these available alongside other architecture information, and provide project teams with a one stop shop for their project planning requirements.

3.7 Solution Architecture Guidance and Oversight

Solution and technical architects engaged by ICT project teams or vendors can be overly focused on the delivery of specific requirements for an isolated business area and may overlook or forget the "big picture" or holistic view and its benefits.

On top of delivering fit-for-purpose solutions, the project also needs to make sure that they are durable, fit well into the environment and aligned to the future state EA. To do this, the project needs to:

- Provide solutions that align to MDA and whole-of-government business strategies.
- Be developed according to agreed principles and standards that instil good practice.
- Complement and integrate well into an existing environment.
- Use technologies and hosting arrangements that will bring down the long-term total cost of ownership, for instance by leveraging existing whole-of-government solutions.

Under GGEA v2.0, involvement of EAs in project planning will provide valuable direction, guidance and oversight for solution architecture in designing solutions and producing deliverables that align with the MDA's strategic direction.

Acting as a central governance function for the organization's architecture, EAs can apply the governance and assurance processes to ensure that project teams deliver designs and implement solutions that align with the agreed architectural outcomes.

3.8 Architecture Patterns and Reusability

A Reference Architecture is one example of a reusable pattern or asset that provides a template solution, prescriptive guidance or a defined set of architectural guidelines and constraints about a specific subject to be shared across an MDA's business process, systems, information and technology. It reflects lessons learned from previous change programmes, offers standardized terminology, provides a common language and encourages adherence to common standards and best practices.

Utilizing an existing reference architecture eliminates the need to reinvent the wheel. More importantly, creating and using a reference architecture will support consistency across solutions and streamlining or reducing potential duplication in addressing the same problems, while simultaneously increasing the chance of delivering successful solutions.

Other types of reusable assets that GGEA v.2.0 will make available include shared services and infrastructures, best practices & guidelines for different activities (system design, software specification and constructions, testing, etc.), solution documents, code fragments, scripts and so on.

The Sector-wide focus on creating, maintaining, identifying and utilizing reusable assets sponsored by GGEA v.2.0 will make a notable contribution to reduced ICT project and operational costs, increased stability and efficiency throughout the project life cycle, while reducing risk.

GGEA v.2.0 will promote the concept of asset reuse, make EAs available to assist with leading and coordinating the collection of reusable assets at the MDA level, and provide a central store to make them available for use across the public sector to benefit other MDAs.

4 ARCHITECTURE GOVERNANCE

To ensure GGEA v.2.0 is sustained and yields the envisioned benefits, it needs to be governed. Making enterprise architecture effective involves the substantial challenge of attempting to affect the behaviour of staff not under direct control, which brings with it considerable difficulties that can undermine the best of efforts. Without Governance, the various MDAs will follow their own policy, guidelines and standards (if any) without alignment to the overall GGEA v.2.0.

Architecture governance is the practice by which EA is managed and controlled at an enterprise-wide level. Architecture governance typically does not operate in isolation, but within a hierarchy of governance structures, which can include all of the following as distinct domains with their own disciplines and processes.

Each of these domains may exist at multiple geographic levels within the overall organization. Governance as a whole is thus a broad topic, beyond the scope of an enterprise architecture such as GGEA v.2.0, however it is important to understand that architecture governance takes place within the context of enterprise-wide governance, because of the hierarchy of governance structures within which it typically operates, as illustrated above.

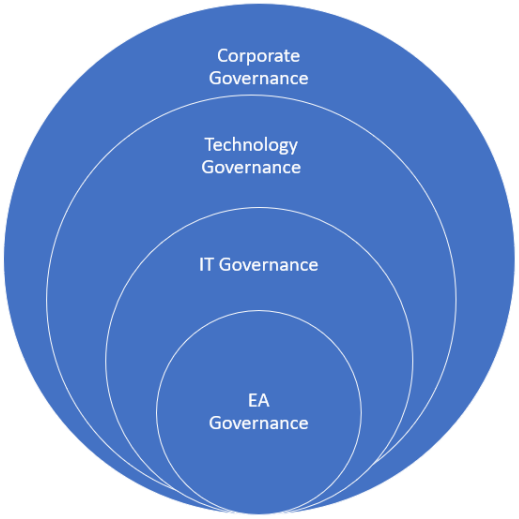

Figure 13 - EA Governance Relative to other Governance Domains

Architecture governance, as a subset of IT Governance, includes the following:

- Implementing a system of controls over the creation and monitoring of all architectural components and activities, to ensure the effective introduction, implementation, and evolution of architectures within the organization
- Implementing a system to ensure compliance with internal and external standards and regulatory obligations
- Establishing processes that support effective management of the above processes within agreed parameters
- Developing practices that ensure accountability to a clearly identified stakeholder community, both inside and outside the organization

Governance will involve certain actors/roles at different milestones, in order to ensure GGEA v.2.0 is followed and is aligned to the overall objectives of GoG.

Periodic review, a key governance function, is critical to determining what is working and what needs improvement. Architecture groups that attempt to move forward without regular feedback on their value to their organization risk dissipating their resources rather than focusing on high-impact areas.

Please see Annex B for a detailed description of the Target State GGEA V.2.0 Governance structure, content and processes.

ANNEXES

Annex A – GGEA v.2.0 Architecture Reference Models

Reference models are the taxonomies that provide standardized categorization to describe MDAs' public sector architecture elements across various viewpoints.

Reference models allow architects within an MDA and across the public sector to communicate using a common language. They support consistent analysis and reporting across MDA and whole-of-government EA functions. Through the use of common reference models and their vocabularies, ICT portfolios can be better managed and leveraged across the public sector, facilitating collaboration and ultimately achieving GoG ICT strategic goals.

The GGEA v.2.0 reference models are specifically designed to provide common taxonomies and categories to describe MDA and whole-of-government architecture and the elements contained within it.

There are six reference models in GGEA v.2.0:

1. **Performance Reference Model (PRM)**
   An outcome-focused measurement framework that can assist in the design and implementation of effective measurements across GGEA v.2.0 domains.
2. **Business Reference Model (BRM)**
   Provides a framework facilitating a whole-of-government functional view of the public sector's Lines of Business and the associated government functions, independent of the MDA performing them.
3. **Service Reference Model (SRM)**
   Business-driven, functional framework classifying services according to how they support business capabilities and performance objectives, facilitating the identification of application components that can be shared across the GoG.
4. **Data Reference Model (DRM)**
   Flexible, standards-based framework that supports information sharing and reuse across the public sector and defines data principles, design and security considerations related to the management of data.
5. **Technology Reference Model (TRM)**
   Component-driven, technical framework categorizing standards and technologies to support and enable the delivery of services and capabilities. Defines the infrastructure technologies and their respective technical standards to enable better system integration and interoperability across the Ghana Government. It also defines the security considerations and standards related to the infrastructure technologies.
6. **Security Reference Model (ScRM)**
   Defines the building blocks of security mechanisms (controls) related to Service and Technology Models, used in the construction and implementation of protective solutions to mitigate risks.

The Figure below depicts the overall GGEA v.2.0 Reference Architecture.

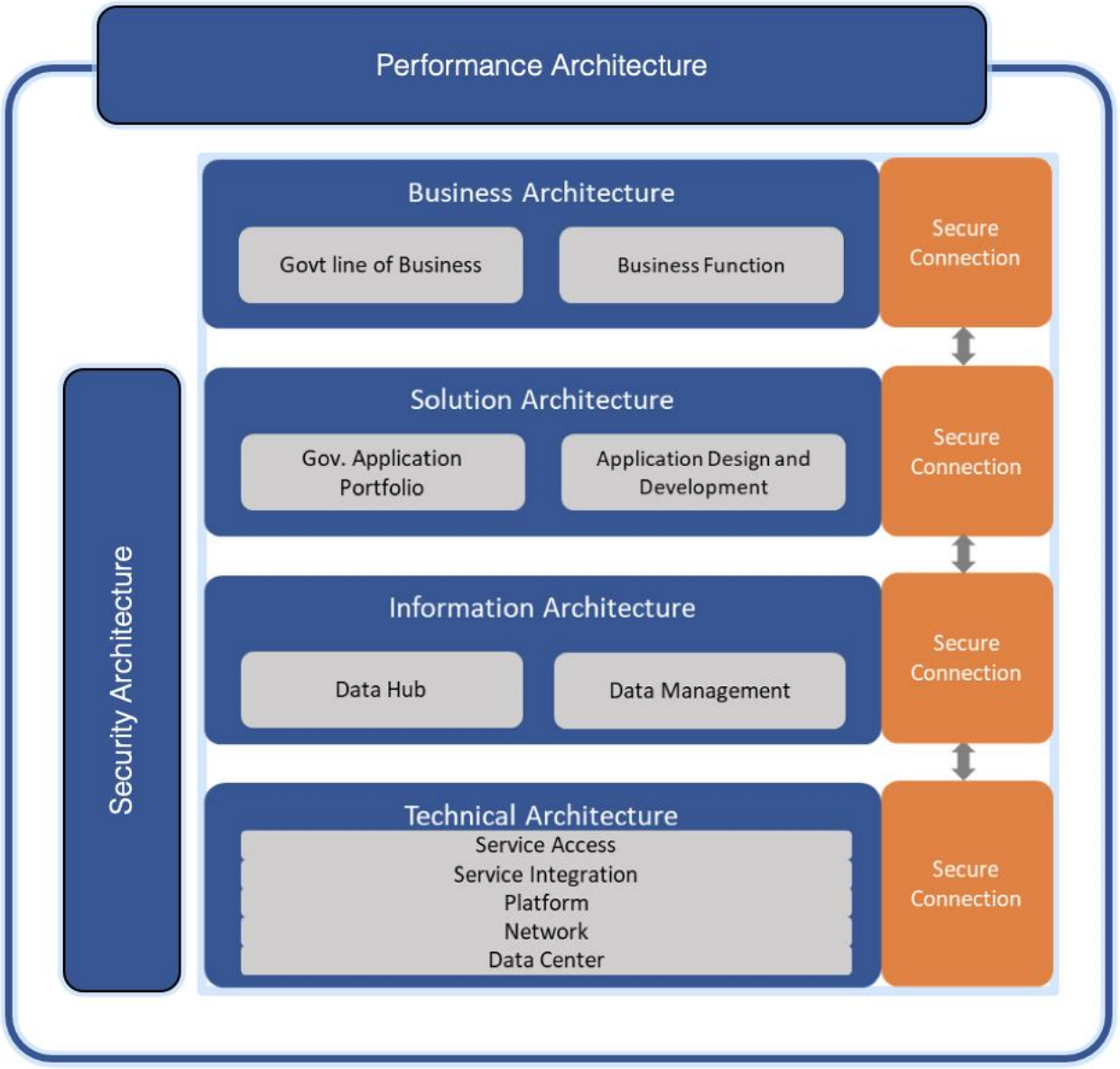

Figure 14 - GGEA v.2.0 Reference Architecture

Annex A1 - GGEA v.2.0 Performance Reference Model

The Performance Reference Model (PRM) has a measurement framework that aligns with the Government of Ghana business operation model. It supports the identification and definition of measures that are able to capture and describe for business:

- the efficiency of MDAs in their utilisation of public funds and resources in the delivery of business outputs;
- the effectiveness of the outputs produced by MDAs in realising desired outcomes for the government and the MDA;
- the overall efficacy (ability to execute) of MDAs and the delivery of government programmes.

When implemented in support of business intelligence systems, balanced scorecards, enterprise architecture or other measurement systems, this framework for measurement delivers to MDA executives a line of sight between the inputs of a business initiative and the realisation of outcomes from that initiative.

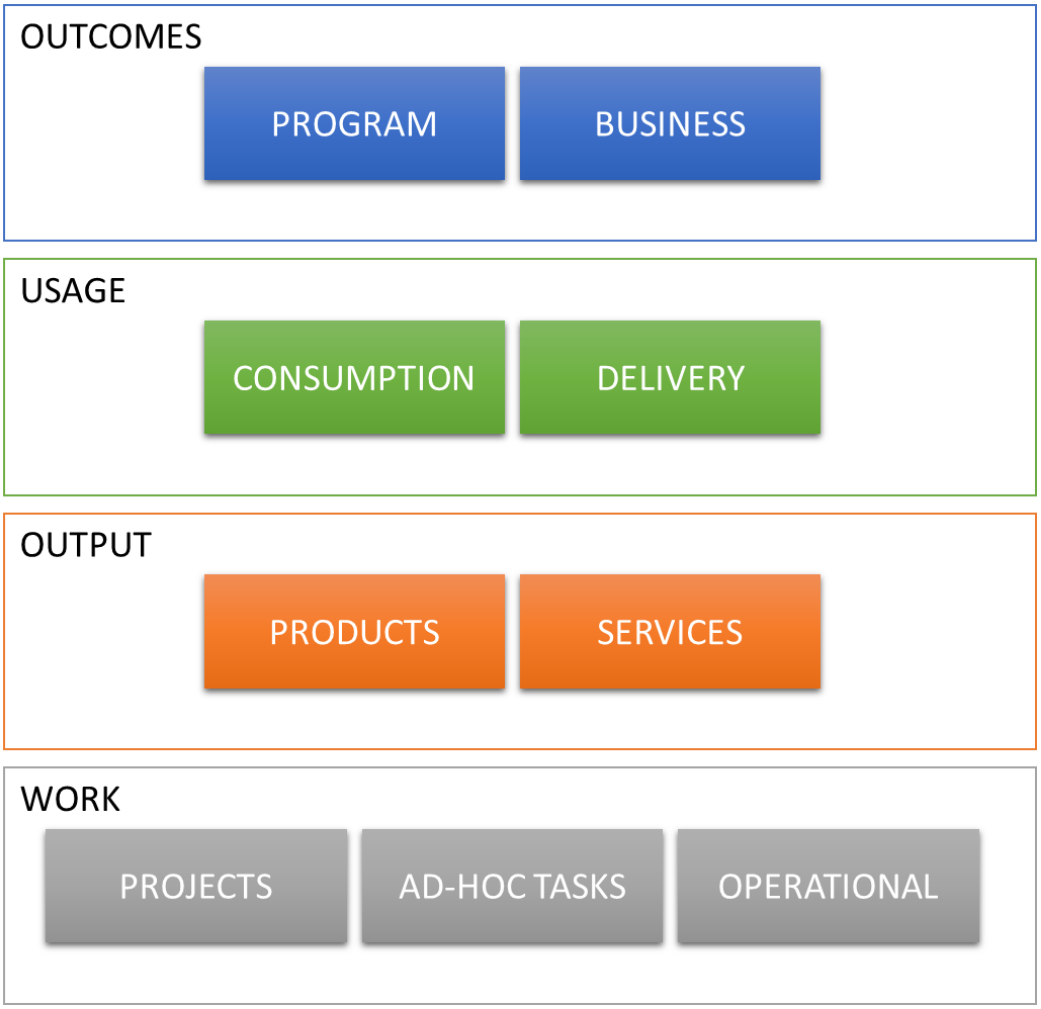

Figure 15 – Performance Reference Model (PRM)

There are four measurement domains within the PRM, and within the four measurement domains there are 9 domain sub-types. Under each of the measurement domain sub-types are groupings for sub-type

attributes that correspond to the characteristics of the domain sub-type, and below the sub-type attributes are measurement groupings that provide further refinement of attributes that possess multiple variables. These are:

1. Outcomes
    a. Programme Outcomes
    The following outcome themes are derived from the functional themes of government set out in GGEA:
        - Governance
        - Finance & Economy
        - Infrastructure
        - Social Services
    b. Business outcomes
    Business outcomes are outcomes that are the targets of MDAs and the whole-of-government in management and operation of the inputs to the business (people, technology, assets, money etc.). The structure of the business outcomes measurement domain sub-type, below the broad-level themes of business operation, will be determined by individual MDAs and the initiatives they define to maintain and improve their performance in those areas of operation:
        - Business management
            - portfolio, programme and project management
            - governance
            - programme administration
            - strategic planning
            - business planning
            - capability planning
            - business continuity
            - legal services
            - human resources
        - Communications management
            - media relations
            - government correspondence
            - internal communications
            - reporting
            - event management
            - publications
            - information & knowledge management
        - Facilities management
            - building and installation management
            - fleet management
            - infrastructure management
            - security management
        - Financial management
            - departmental funding
            - departmental investment management
            - employee remuneration agreements

- budget management
- procurement

2. Usage

   Usage is the mechanism by which the outputs produced by a business initiative realise the outcomes of the initiative. Without some form of usage by a citizen or business, the outputs of government programmes, projects and processes will be unable to realise any form of benefit for an MDA.

   a. Product consumption
      i. Timeliness
      ii. Accessibility
      iii. Consumption
      iv. Coverage
      v. Effectiveness
   b. Service delivery
      i. Availability
      ii. Coverage
      iii. Effectiveness
      iv. Accessibility
      v. Timeliness and responsiveness

3. Outputs

   Outputs of processes and activities can take one of two forms: a new artefact or an altered artefact. An artefact is any physical or virtual entity that is created or sustained as the result of processes and activities being executed within an MDA. The outputs of work are intended to be made available for consumption and utilisation by targeted constituents (citizens or businesses). Outputs are the interfaces and mechanisms through which the government provides services for citizens or businesses.

   a. Products
      i. Fit for Purpose
      ii. Product value
   b. Services
      i. Fit for Purpose

4. Work

   'Work' is the general term applied to the business processes and activities executed within MDAs. Work is the conversion of input resources into outputs via processes. There are only three different types of work:

   a. Projects

      Projects have a long duration, are intended to realise change (achieve an outcome), have highly formalised control structures (governance), and by definition are executed only once. The following are classifications of project performance:
      i. Project efficiency
      ii. Project control
      iii. Project adaptability
      iv. Complexity
      v. Project safety
   b. Ad-hoc tasks

Ad hoc tasks have a typically short duration period and largely informal control structures. They can occur as a one-time activity or on a regular basis and may have the ability to change an organisation, but that is undesirable for the organisation. The following are classifications of ad-hoc tasks performances:

i. Task efficiency
ii. Task safety
iii. Task complexity

c. Processes and operations

Operations and business as usual (BAU) are often referred to as processes and may have a short or long duration. They have highly formalised control structures (rules and governance), are highly repetitive and are designed specifically to not realise change. The following are classifications of processes and operations performance:

i. Process efficiency
ii. Process control
iii. Process availability
iv. Process complexity
v. Process adaptability
vi. Process maturity
vii. Process safety
viii. Process reliability

Annex A2 - GGEA v.2.0 Business Reference Model

The BRM is the first layer of GGEA v.2.0 at the whole-of-government level. It is the main viewpoint for the analysis of data, applications and their capabilities, and the implementation of technologies to support reuse and standards. This framework should be used by MDAs when identifying and building their architectures to ensure that investments leverage existing components, applications, and services across the whole-of-government.

The Objectives of the BRM are:

a. To provide a context and a framework for defining / redefining the Enterprise Vision, Goals and Objectives;
b. To describe the customers and the channels they use to interact with the government.
c. To delineate the Scope of the Enterprise Architecture effort;
d. To identify the broad parameters on which to assess the performance of the enterprise and the success of its endeavour;
e. To describe the portfolio of services and functions, which include the existing and new;
f. To enable preparation of a role-responsibility matrix;
g. To identify the broad areas requiring process re-engineering and recommend methods for undertaking the same;
h. To enable the enterprise to redesign its organizational structure(s) to meet its Goals and Objectives better and in a coordinated, joined-up manner.

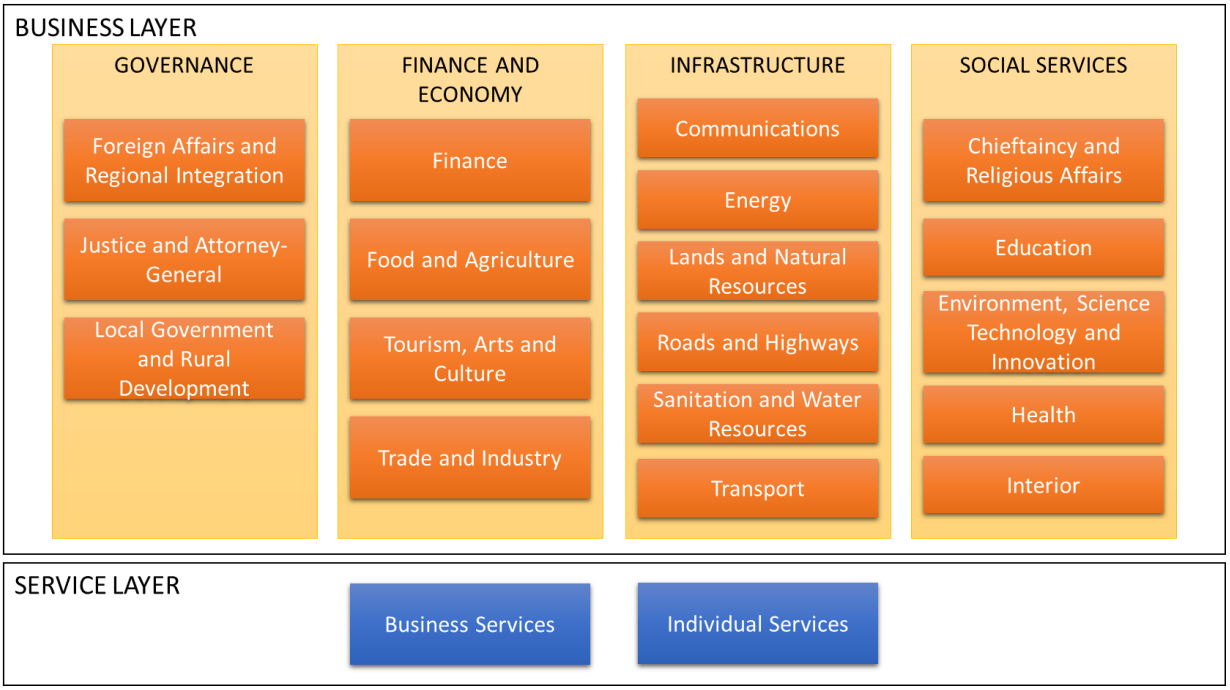

Figure 16 – Business Reference Model (BRM)

BRM Structures are composed of:

1. Business Layer
    a. Governance
        i. Foreign Affairs and Regional Integration
            - Passport Office
        ii. Justice and Attorney-General
            - Council For Law Reporting
            - Ghana Copyright Office
            - Ghana School of Law
            - Registrar General's Department
            - The Judicial Service of Ghana
        iii. Local Government and Rural Development
            - Ablekuma Central Municipal Assembly
            - Ablekuma North Municipal Assembly
            - Ablekuma South Municipal Assembly
            - Ablekuma West Municipal Assembly
            - Accra Metropolitan Assembly
            - Ada East Municipal Assembly
            - Ada West Municipal Assembly
            - Adentan Municipal Assembly
            - Ashaiman Municipal Assembly
            - Ayawaso Central Municipal Assembly
            - Ayawaso East Municipal Assembly
            - Ayawaso North Municipal Assembly
            - Ayawaso West Municipal Assembly
            - Births And Deaths Registry
            - Department Of Community Development
            - Department Of Parks And Gardens
            - Ga Central Municipal Assembly
            - Ga East Municipal Assembly
            - Ga North Municipal Assembly
            - Ga South Municipal Assembly
            - Ga West Municipal Assembly
            - Korle Klottey Municipal Assembly
            - Kpone Katamanso Municipal Assembly
            - Krowor Municipal Assembly
            - La Dade-Kotopon Municipal Assembly
            - La Nkwantanan Municipal Assembly
            - Ledzokuku Municipal Assembly
            - Ningo Prampram Municipal Assembly
            - Okaikwei North Municipal Assembly
            - Shai Osudoku Municipal Assembly
            - Tema Metropolitan Assembly
            - Tema West Municipal Assembly
            - Weija-Gbawe Municipal Assembly
    b. Finance and Economy
        i. Finance

- Association of Customs House Agents of Ghana
- Ghana Revenue Authority
- Institute of Accountancy Training
- National Pensions Regulatory Authority
- Public Procurement Authority (Ppa)
- Securities and Exchange Commission

ii. Food and Agriculture
- Animal Production Directorate
- Fisheries Commission of Ghana
- Ghana Cocoa Board
- National Premix Fuel Secretariat
- Veterinary Service Directorate

iii. Tourism, Arts and Culture
- Ghana Trade Fair Company Limited
- Creative Arts Agency
- Ghana Museums and Monuments Board (Gmmb)
- Ghana Tourism Authority
- Hotel, Catering and Tourism Training Institute
- Kwame Nkrumah Memorial Park
- National Folklore Board
- National Sport Authority
- National Theatre of Ghana
- W.E.B. Dubois Memorial Centre for Pan African Culture

iv. Trade and Industry
- Customs Broker Association of Ghana
- Ghana Export Promotion Authority (GEPA)
- Ghana Institute of Freight Forwarders
- Ghana International Trade Commission
- Ghana Investment Promotion Centre
- Ghana National Chamber of Commerce
- Ghana Standards Authority (GSA)
- Gihoc Distilleries Company Ltd
- Gratis Foundation
- Volta Star Textiles Limited

c. Infrastructure

i. Communications
- Advanced Information Technology Institute- Kofi Annan Centre of Excellence (AITI-KACE)
- Data Protection Commission (DPC)
- Ghana Meteorological Agency
- Ghana News Agency
- Ghana Post Company
- Information Services Department
- National Communications Authority
- National Information Technology Agency (NITA)
- Postal and Courier Services Regulatory Commission (PCSRC)

ii. Energy
    - Electricity Company of Ghana
    - Energy Commission
    - Ghana National Petroleum Corporation
    - National Biosafety Authority
    - National Petroleum Authority
    - Nuclear Regulatory Authority
    - Valco Trust Fund

iii. Lands and Natural Resources
    - Hydrological Services Department
    - Lands Commission
    - Minerals Commission Ghana
    - Minerals Development Fund
    - Rent Control Department
    - State Housing Company Limited

iv. Roads and Highways
    - Department of Feeder Roads
    - Ghana Railway Development Authority

v. Sanitation and Water Resources
    - Architects Registration Council
    - Community Water and Sanitation Agency
    - Ghana Water Company Limited (GWCL)
    - Water Resources Commission

vi. Transport
    - Driver and Vehicle Licensing Authority
    - Freight Forwarders Association of Ghana
    - Ghana Highway Authority
    - Ghana Railway Company Limited
    - Ghana Road Fund Secretariat
    - Ghana Shippers Authority
    - Government Technical Training Centre
    - Metro Mass Transit Limited
    - National Road Safety Authority

d. Social Services

i. Chieftaincy and Religious Affairs
    - Chieftaincy and Religious Affairs

ii. Education
    - Centre for National Distance Learning and Open Schooling
    - Commission for Technical and Vocational Education and Training (CTVET)
    - Department of Co-Operatives
    - Department of Factories Inspectorate
    - Department of Rural Housing
    - Ghana Commission for UNESCO
    - Ghana Free Zones Authority
    - Ghana National Service Scheme (NSS)

- Ghana Psychology Council
- Ghana Scholarships Secretariat
- Jetstream Technologies Limited
- Management Development and Productivity Institute
- National House of Chiefs
- National Schools Inspectorate Authority
- National Vocational Training Institute
- National Youth Authority
- Precious Minerals Marketing Company Limited
- Student Loan Trust Fund
- TDC Development Company Limited
- Veterans Administration of Ghana

iii. Environment, Science, Technology and Innovation
- Biotechnology and Nuclear Agriculture Research Institute
- Council For Scientific and Industrial Research
- Environmental Protection Agency
- Ghana Atomic Energy Commission
- Radiation Protection Institute

iv. Health
- Centre for Plant Medicine Research
- Food and Drugs Authority
- Ghana College of Nurses and Midwives
- Ghana College of Physicians and Surgeons
- Ghana Health Service
- Korle Bu Teaching Hospital
- National Ambulance Service
- National Blood Service
- Pharmacy Council

v. Interior
- Gaming Commission of Ghana
- Ghana Immigration Service
- Ghana National Fire Service
- National Disaster Management Organisation

2. Service Layer
   a. Business Services
      i. Business Registrations and Permits
         - Set up a Business
         - Manage Statutory Filings and Permits
      ii. Driving and Transportation
         - Get a Driving Licence
         - Road Worthy Certificates
         - Register a Vehicle
      iii. Education, Science and Technology
         - Apply for a Student Loan

- License an Educational Institution

iv. Energy and Petroleum
- Apply for Certificates
- Electricity
- Other Licences

v. Environment
- EPA
- Sanitation
- Recycling
- Eco-services

vi. Health and Food Services
- Medical services
- Food
- Drugs and Pharmaceutical Standards

vii. Housing, Land and Local Services
- Land Registration
- Land Title
- Rent Control

viii. Money and Finance
- Income
- Personal
- Corporate Taxes

ix. Other
- Other services provided by the Government of Ghana

x. Police, Justice and Safety
- Contact the Police
- Start a Legal Case
- Contact Security Services

xi. Social Services and Welfare
- Includes social services and interventions by the Government of Ghana

xii. Visas and Immigration
- Work, stay or live in Ghana

xiii. Working, Employment and Pensions
- Manage your pension

b. Individual Services

i. Births, Deaths & Marriages
- Apply for Birth, Death, Marriage and Divorce Certificates

ii. Business Registrations and Permits
- Set up a Business
- Manage Statutory Filings and Permits

iii. Driving and Transportation
- Get a Driving Licence
- Road Worthy Certificates
- Register a Vehicle

iv. Education, Science and Technology
- Apply for a Student Loan

- License an Educational Institution

v. Energy and Petroleum
   - Apply for Certificates
   - Electricity
   - Other Licences

vi. Environment
   - EPA
   - Sanitation
   - Recycling
   - Eco-services

vii. Health and Food Services
   - Medical services
   - Food
   - Drugs and Pharmaceutical standards

viii. Housing, Land and Local Services
   - Land Registration
   - Land Title
   - Rent Control

ix. Money and Finance
   - Income
   - Personal
   - Corporate Taxes

x. Other
   - Other services provided by the Government of Ghana

xi. Police, Justice and Safety
   - Contact the Police
   - Start a Legal Case
   - Contact Security Services

xii. Social Services and Welfare
   - Includes social services and interventions by the Government of Ghana

xiii. Visas and Immigration
   - Work, stay or live in Ghana

xiv. Working, Employment and Pensions
   - Manage your pension

Annex A3 - GGEA v.2.0 Service Reference Model

The Service Reference Model (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 MDAs and their investments and assets. The model aids in recommending service capabilities to support the re-use of business components and services across the Government of Ghana.

The SRM has been structured across service areas that, independent of the business functions, can provide a foundation for the sharing and re-use of applications, application capabilities, components and business services. The following figure depicts the Service Reference Model for Ghana.

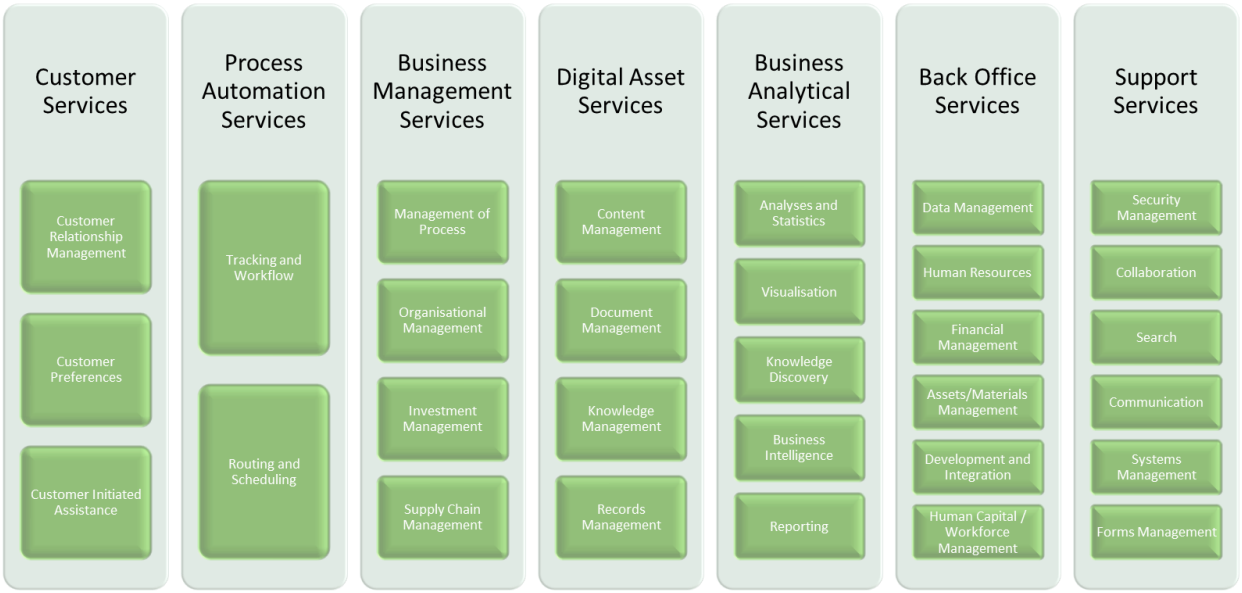

Figure 17 – Service Reference Model (SRM)

SRM Structures are composed of:

1. Customer Services
    a. Customer Relationship Management
        i. Call Centre Management
        ii. Customer Analytics
        iii. Sales and Marketing
        iv. Product Management
        v. Brand Management
        vi. Customer/Account Management
        vii. Contract and Profile Management
        viii. Partner Relationship Management
        ix. Customer Feedback
        x. Surveys

   b. Customer Preferences
      i. Personalisation
      ii. Subscriptions
      iii. Alerts and Notifications
   c. Customer Initiated Assistance
      i. Online Help
      ii. Online Tutorials
      iii. Self-Service
      iv. Reservations/Registration
      v. Multi-Lingual Support
      vi. Assistance Request
      vii. Scheduling
2. Process Automation Services
   a. Tracking and Workflow
      i. Process Tracing
      ii. Case Management
      iii. Conflict Resolution
   b. Routing and Scheduling
      i. Inbound Correspondence Management
      ii. Outbound Correspondence Management
3. Business Management Services
   a. Management of Process
      i. Change Management
      ii. Configuration Management
      iii. Requirements Management
      iv. Programme / Project Management
      v. Governance / Policy Management
      vi. Quality Management
      vii. Business Rule Management
      viii. Risk Management
   b. Organisational Management
      i. Workgroup / Groupware
      ii. Network Management
   c. Investment Management
      i. Strategic Planning & Management
      ii. Portfolio Management
      iii. Performance Management
   d. Supply Chain Management
      i. Procurement
      ii. Sourcing Management
      iii. Inventory Management
      iv. Catalogue Management
      v. Ordering / Purchasing
      vi. Invoice / Requisition Tracking and Approval
      vii. Storefront / Shopping Cart
      viii. Warehouse Management

ix. Returns Management
x. Logistics and Transportation

4. Digital Asset Services
    a. Content Management
        i. Content Authoring
        ii. Content review and Approval
        iii. Tagging and Aggregation
        iv. Content Publishing and Delivery
        v. Syndication Management
    b. Document Management
        i. Document Imaging and OCR
        ii. Document Referencing
        iii. Document Revisions
        iv. Library / Storage
        v. Document Review and Approval
        vi. Document Conversion
        vii. Indexing
        viii. Classification
    c. Knowledge Management
        i. Information Retrieval
        ii. Information Mapping / Taxonomy
        iii. Information Sharing
        iv. Categorisation
        v. Knowledge Engineering
        vi. Knowledge Capture
        vii. Knowledge Distribution and Delivery
        viii. Smart Documents
    d. Records Management
        i. Record Linking / Association
        ii. Document Retirement
        iii. Digital Rights Management
5. Business Analytical Services
    a. Analyses and Statistics
        i. Mathematical
        ii. Structural / Thermal
        iii. Radiological
        iv. Forensics
    b. Visualisation
        i. Graphic / Charting
        ii. Imagery
        iii. Multimedia
        iv. Mapping / Geospatial / Elevation / GPS
        v. CAD
    c. Knowledge Discovery
        i. Data Mining
        ii. Modelling

iii. Simulation
- d. Business Intelligence
  - i. Demand Forecasting / Management
  - ii. Balanced Scorecard
  - iii. Decision Support and Planning
- e. Reporting
  - i. Ad hoc
  - ii. Standardised / Canned
  - iii. OLAP

6. Back Office Services
   - a. Data Management
     - i. Data Exchange
     - ii. Data Mart
     - iii. Data Warehouse
     - iv. Metadata Management
     - v. Data Cleansing
     - vi. Extraction and Transformation
     - vii. Loading and Archiving
     - viii. Data Recovery
     - ix. Data Classification
   - b. Human Resources
     - i. Recruiting
     - ii. Resume Management
     - iii. Career Development and Retention
     - iv. Time Reporting
     - v. Awards Management
     - vi. Benefit Management
     - vii. Retirement Management
     - viii. Personnel Administration
     - ix. Education / Training
     - x. Health and Safety
     - xi. Travel Management
   - c. Financial Management
     - i. Billing and Accounting
     - ii. Credit / Charge
     - iii. Expense Management
     - iv. Payroll
     - v. Payment / Settlement
     - vi. Debt Collection
     - vii. Revenue Management
     - viii. Internal Controls
     - ix. Auditing
     - x. Activity-based Management
     - xi. Currency Translation
   - d. Assets/Materials Management
     - i. Property / Asset Management

ii. Asset Cataloguing / Identification
iii. Asset Transfer, Allocation and Maintenance
iv. Facilities Management
v. Computers / Automation Management

e. Development and Integration
i. Legacy Integration
ii. Enterprise Application Integration
iii. Data Integration
iv. Instrumentation and Testing
v. Software Development

f. Human Capital / Workforce Management
i. Resource Planning and Allocation
ii. Skills Management
iii. Workforce Directory / Locator
iv. Team / Organisation Management
v. Contingent Workforce Management
vi. Workforce Acquisition / Optimisation

7. Support Services
a. Security Management
i. Identification and Authentication
ii. Access Control
iii. Cryptography
iv. Digital Signature Management
v. Intrusion Prevention
vi. Intrusion Detection
vii. Incident Response
viii. Audit Trail Capture and Analysis
ix. Certification and Accreditation
x. ISM Management and Reporting
xi. Virus Protection

b. Collaboration
i. Email
ii. Threaded Discussions
iii. Document Library
iv. Shared Calendaring
v. Task Management
vi. Social Networking

c. Search
i. Query
ii. Precision/Recall Ranking
iii. Classification
iv. Pattern Matching

d. Communication
i. Real Time/Chat
ii. Instant Messaging
iii. Audio Conferencing

iv. Video Conferencing
v. Event/News Management
vi. Community Management
vii. Computer/Telephony Integration
viii. Voice Communications

e. Systems Management
i. License Management
ii. Remote Systems Control
iii. System Resource Monitoring
iv. Software Distribution
v. Issue Tracking

f. Forms Management
i. Forms Creation
ii. Forms Modification

Annex A4 - GGEA v.2.0 Data Reference Model

The Data Architecture Reference Model (DRM) is a flexible and standards-based framework to enable information sharing and reuse across the Government via the standard description and discovery of common data and the promotion of uniform data management practices. The DRM provides a standard means by which data may be described, categorised, and shared.

Data Architecture is fundamental to data management. Because most organizations have more data than individual people can comprehend, it is necessary to represent organizational data at different levels of abstraction so that it can be understood and management can make decisions about it.

Data Architecture artefacts includes specifications used to describe existing state, define data requirements, guide data integration, and control data assets as put forth in a data strategy. An organization's Data Architecture is described by an integrated collection of master design documents at different levels of abstraction, including standards that govern how data is collected, stored, arranged, used, and removed. It is also classified by descriptions of all the containers and paths that data takes through an organization's systems.

The most detailed Data Architecture design document is a formal enterprise data model, containing data names, comprehensive data and Metadata definitions, conceptual and logical entities and relationships, and business rules. Physical data models are included, but as a product of data modelling and design, rather than Data Architecture.

Data Architecture is most valuable when it fully supports the needs of the entire enterprise. Enterprise Data Architecture enables consistent data standardization and integration across the enterprise.

The artefacts that architects create constitute valuable Metadata. Architectural artefacts should be stored and managed in the GGEA v.2.0 artefact Repository.

The data architecture principles below apply to all MDAs in terms of how they use and manage data.

Principle 1: Data is an Asset

Data is an asset that has value to Government and is managed accordingly.

Rationale:
Data is a valuable Government resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision making. Accurate, timely data is critical to accurate, timely decisions. Most government assets are carefully managed, and data is no exception.
Because data is the foundation of decision making, MDAs must carefully manage data to assure that they know where it is, can rely upon its accuracy, and can obtain it when and where we need it.
Implications:

- This is one of three closely related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organisations within the Enterprise understand the relationship between value of data, sharing of data, and accessibility to data.

- Stewards must have the authority and means to manage the data for which they are accountable.
- MDAs must make the cultural transition from "data-ownership" thinking to "data-stewardship" thinking.
- The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to NITA personnel and adversely affect decisions across the Government of Ghana.
- Part of the role of data steward, who manages the data, is to ensure data quality. Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality – it is probable that policy and procedures will need to be developed for this as well.
- A forum with comprehensive Government-wide representation should decide on process changes suggested by the steward.
- Since data is an asset of value to the entire Government, data stewards accountable for properly managing the data must be assigned at the Government level.

Principle 2: Data is Shared

Users have access to the data necessary to perform their duties; therefore, data is shared across Government functions and organisations.

Rationale:

Timely access to accurate data is essential to improving the quality and efficiency of Government decision making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The Government holds a wealth of data, but it is stored in hundreds of incompatible stovepipe/silo databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organisation to efficiently share these islands of data across the organisation.

Shared data will result in improved decisions since MDAs will rely on fewer (ultimately, one virtual) sources of more accurate and timely managed data for all their decision making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.

Implications:

- This is one of three closely related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organisations within Government understand the relationship between value of data, sharing of data, and accessibility to data.
- To enable data sharing MDAs must develop and abide by a common set of policies, procedures and standards governing data management and access for both the short and the long term.
- For the short term, to preserve their significant investment in legacy systems, MDAs must invest in software capable of migrating legacy system data into a shared data environment.

- MDAs will also need to develop standard data models, data elements, and other metadata that defines this shared environment, and develop a repository system for storing this metadata to make it accessible.
- For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications.
- For both the short term and the long term MDAs must adopt common methods and tools for creating, maintaining and accessing the data shared across the Government
- Data sharing will require a significant cultural change.
- This principle of data sharing will continually "bump up against" the principle of data security. Under no circumstances should the data sharing principle cause confidential data to be compromised.
- Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision making. Shared data will become the Government-wide "virtual single source" of data.

Principle 3: Data is Accessible

Data is accessible for users to perform their functions

Rationale:
Wide access to data leads to efficiency and effectiveness in decision-making and affords timely response to information requests and service delivery. Using information must be considered from a Government perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved.
Implications:

- This is one of three closely related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all MDAs understand the relationship between value of data, sharing of data, and accessibility of the data.
- Accessibility involves the ease with which users obtain information.
- The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of Government users and their corresponding methods of access.
- Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information.
- Access to data does not necessarily grant the user access rights to modify or disclose the data. This will require an education process and a change in the culture, which currently supports a belief in "ownership" of data by functional units

Principle 4: Data Steward/Trustee

Each data element has a steward/trustee accountable for data quality.

Rationale:
One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across Government. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data steward/trustee makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the data steward/trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources.
Implications:

- Real stewardship/trusteeship dissolves the data "ownership" issues and allows the data to be available to meet all users' needs.
- The data steward/trustee will be responsible for meeting quality requirements levied upon the data for which the steward/trustee is accountable.
- It is essential that the steward/trustee has the ability to provide user confidence in the data based upon attributes such as 'data source.'
- It is essential to identify the true source of the data in order that the data authority can be assigned this stewardship/trusteeship responsibility. This does not mean that classified sources will be revealed nor does it mean the source will be the steward/trustee.
- Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data.
- As a result of sharing data across Government, the steward/trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and subsequently, must then recognise the importance of this stewardship/trusteeship responsibility.

Principle 5: Common Vocabulary and Data Definitions

Data is defined consistently throughout the Enterprise, and the definitions are understandable and available to all users.

Rationale:
The data that will be used in the development of applications must have a common definition throughout the Government to enable sharing of data. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.
Implications:

- Significant resources must be committed to this task. It is a key to the success of efforts to improve the information environment. This is separate from but related to the issue of data element definition, which is addressed by a broad community - this is more like a common vocabulary and definition.
- The Government must establish the initial common vocabulary for the business. The definitions will be used uniformly throughout the MDAs:
- Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the Government metadata descriptions.

- Ambiguities resulting from multiple parochial definitions of data must give way to accepted Government-wide definitions and understanding.
- Multiple data standardisation initiatives need to be coordinated.
- Functional data administration responsibilities must be assigned

Principle 6: Data Security

Data is protected from unauthorised use and disclosure.

Rationale:
Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information. Existing laws and regulations require the safeguarding of national security and the privacy of data, while permitting free and open access.
Implications:

- Aggregation of data both classified and not, will create a large target requiring review and declassification procedures to maintain appropriate control.
- Data owners and/or functional users must determine if the aggregation results in an increased classification level. MDAs will need appropriate policy and procedures to handle reviews and declassification. Access to information based on a need-to-know policy will force regular reviews of the body of information.
- The current practice of having separate systems to contain different classifications needs to be rethought. Is there a software solution to separating classified and unclassified data? The current hardware solution is unwieldy, inefficient, and costly. It is more expensive to manage unclassified data on a classified system.
- Currently, the only way to combine the two is to place the unclassified data on the classified system, where it must remain.
- In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level.
- Data security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity labelling for access to information must be determined.
- Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorised access and manipulation.

The Data Architecture Reference Model (DRM) describes the main entities that the Government is involved with, and on which data is stored in Government systems or archives, and the main properties, or data items, stored for each entity. These entities participate in different processes, which were described in the Business Architecture Reference Model (BRM). Thus, the BRM and DRM together provide a complete set of system analysis views of the Government of Ghana, by depicting both the main processes and the main entities involved in those processes.

The main purpose of the DRM is to provide a common dictionary, or language, describing the main data entities in Government, and specifically those data entities shared across MDAs. This dictionary will serve as the infrastructure, on which later master data management, data sharing and data exchange

mechanisms may be built. For example, it is impossible to define mechanisms by which data from the national population registry regarding each person such as his name, National ID, Date of Birth and current address are shared or provided to other MDAs, before the ‗person' entity and its main attributes are defined and agreed upon across Government.

It is also desirable that common entities and entity attributes, shared across different MDAs, will be recorded and represented in a uniform manner, across the GoG. Thus, for example, we would like to have one standard way of recording an address, a person's name, or a national ID number. One of the DRM aims is to underlie the infrastructure with those standards.

Thus, the DRM provides a common data dictionary, as well as guidance on using it, to Enterprise Architects and Data Architects for implementing repeatable processes to enable data sharing within the GoG and between the GoG and other organisations. These data sharing processes encompass national and local Governments, as well as other public and private non-Governmental institutions.

Another important role of the DRM is to provide the data context, which means to explain how the different data entities fit within the larger picture of the GGEA v.2.0. The data context is provided through two main venues:

- The first one is tying each data entity to the business functions and lines of business it is related to, thus also tying the DRM to the BRM;
- The other is to provide the context of a specific entity with relation to the other data entities, and this is provided through UML diagrams.

The DRM also includes an abstract framework, or 'meta-model', from which concrete DRM may be derived. This meta-model is designed to facilitate a common approach to Data Architecture which can then be used across the GoG. It should also serve as a means to facilitate communications between NITA and data architects in different MDAs.

The main element in the meta-model is the entity. An entity is any real world 'thing' that we want to keep data on. A person, an organisation, a criminal law case, a budget appropriation, a facility, and a tract of land are all entities. An entity has attributes or data elements. Possible attributes are name, ID or date. It should be possible to record each attribute in a single, or a finite, small number of fields in relational database tables. More complex attributes should be made entities. A data element has a type (such as a string, date or integer) and a Data Description, such as 'a number between 1 and 100'.

Each entity is described by metadata, which is especially relevant for documents and records and includes, among others, the author, audience, subject and last modification date of the document or record. An important aspect of metadata is access rights, how you may modify the data, and who has read only access to the data.

Data may be exchanged, or transferred, between parties, or stakeholders, using messages. A message is composed of data elements, and has an originating stakeholder, or a producer and a receiving stakeholder, or a consumer. A message is exchanged using a message exchange mechanism. As explained in the e-Government Interoperability Framework (eGIF), we envision two main message exchange mechanisms for the GoG, Web Services for online transactions and batch XML files for offline processing.

An entity may be related to other entities. The two main types of relationships, covered in the DRM, are 'is a' or 'derived from', and 'has a'. Thus, for example, an employee is a person, and thus the employee entity is derived from the person entity. This means that the employee entity has all of the person entity attributes and relationships, in addition to a few unique attributes and relationships of its own. The 'has a' relationship denotes lines of responsibility or ownership – an MDA‘s has a budget, employees, facilities and projects.

For each entity we maintain a master data store. For each master data store there is an MDA‘s responsible for maintaining it. One of the purposes of the DRM is to identify the master data store for each entity, and to clearly identify which MDA is responsible for maintaining which data. Data duplication and data maintenance at multiple locations may lead to inconsistencies and inefficiencies. Fraudulent parties may also take advantage of it in order to evade tax payments or make false claims for benefits. Thus, for example, personal identification and contact details data such as name, date of birth, national ID number and current address, will be maintained by the National Registry. Other MDAs may have read access only to the data. This read access may be provided either in the form of a Web Service, or in a process that will duplicate the information stored in the master data store into read only copies located at other MDAs. Recent incidents in the U.K., where the lack of a central National Registry data store made it possible for fraudulent parties to claim millions of pounds in false child benefits, clearly demonstrate why a master data store is required.

Each entity is involved in one or more business processes. Those are, in turn, related to the functions, sub lines of business and lines of business of the Government.

The goal of Data Architecture is to be a bridge between business strategy and technology execution. As part of Enterprise Architecture, Data Architects:

- Strategically prepare organizations to quickly evolve their products, services, and data to take advantage of business opportunities inherent in emerging technologies
- Translate business needs into data and system requirements so that processes consistently have the data they require
- Manage complex data and information delivery throughout the enterprise
- Facilitate alignment between Business and IT
- Act as agents for change, transformation, and agility

Data architects create and maintain organizational knowledge about data and the systems through which it moves. This knowledge enables an organization to manage its data as an asset and increase the value it gets from its data by identifying opportunities for data usage, cost reduction, and risk mitigation.

Data and enterprise architecture deal with complexity from two viewpoints:

- Quality-oriented: Focus on improving execution within business and IT development cycles. Unless architecture is managed, architecture will deteriorate. Systems will gradually become more complex and inflexible, creating risk for an organization. Uncontrolled data delivery, data copies, and interface ‘spaghetti’ relationships make organizations less efficient and reduce trust in the data.

- Innovation-oriented: Focus on transforming business and IT to address new expectations and opportunities. Driving innovation with disruptive technologies and data uses has become a role of the modern Enterprise Architect.

An Enterprise Data Architecture practice generally includes the following work streams, executed serially or in parallel:

- Strategy: Select frameworks, state approaches, develop roadmap
- Acceptance and culture: Inform and motivate changes in behaviour
- Organization: Organize Data Architecture work by assigning accountabilities and responsibilities
- Working methods: Define best practices and perform Data Architecture work within development projects, in coordination with Enterprise Architecture
- Results: Produce Data Architecture artefacts within an overall roadmap

Data architecture is used to find out what data is used in business processes or services or stand-alone data. The data must have the following principles:

1) Data must be collected and maintained in an integrated manner to support needs;
2) Data is a renewable and reusable asset;
3) Data must have the highest possible quality and integrity to be used in making decisions;
4) Data should be stored or placed in the most suitable structure and location for optimal utilization;
5) Data that is dynamic in nature must be updated from time to time;
6) Data must be able to be shared for common needs.

Data and information includes all types of data and information owned by IPPD, and/or obtained from the public, business actors, and/or other parties.

The data and information architecture domain has a direct relationship with the business process domain as the source of the data and information and the infrastructure architecture domain in which the data storage media is classified. All data will be stored in Data Storage which can be accessed and shared according to the rules that have been set.

The GGEA reference models are specifically designed to provide common taxonomies and categories to describe Ghane MDA architecture and the elements contained within it. Figure below shows the taxonomy of data used in DRM for Ghana.

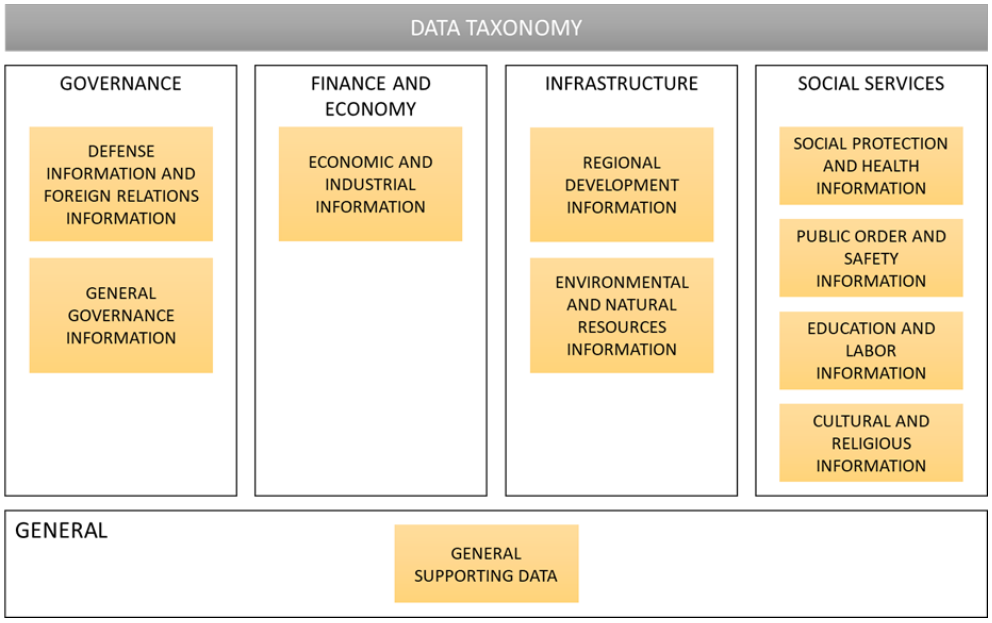

Figure 18 – Data Reference Model (DRM)

The data taxonomy for GoG consists of

1. Governance Data
    a. Defense Information and Foreign Relations Information
        i. Defense data
        Data that presents the field of national defence, including the management of strategic installations and defence potential, defence strategies, countering threats, cyber defence.
        ii. Foreign relations data
        Data representing the field of foreign relations and foreign policy
    b. General Government Information
        i. Domestic data
        Data that represents domestic affairs include political policies, general government, regional autonomy development, regional government, and national priority programmes.
        ii. Financial data
        Data that represents the field of state finance
        iii. Information management data
        Data representing the field of information includes the management of information resources and equipment, public radio broadcasting, and public television broadcasting
        iv. Communication data
        Data that represents the field of communication include public communication, postal administration, and management of postal resources and equipment.
        v. National development planning data
        Data representing the field of national development planning includes monitoring of development deviations, macroeconomic management, and strategic support for programmes/policies.

vi. Employee data
Data that presents the field of employee including public service management, electronic-based government system management, national archives, and inter-MDA collaboration
vii. State secretarial data
Data that represents the field of state secretariat includes relations with State Institutions, management of national security, and government supervision.
viii. Land data
Data representing the land sector includes land litigation and land infrastructure management.
ix. Population data
Data that represents the population sector includes legal assistance in the context of population control and family planning as well as empowering community participation.

2. Finance and Economy Data
    a. Economic and Industrial Information
        i. Industry data
        Data that presents the field of domestic industrial development, including the management of the creative economy and digital products.
        ii. Trading data
        Data that represents trade management includes domestic trade, export-import, and futures trading.
        iii. Agricultural data
        Data that represents the agricultural sector include increased agricultural production, provision of agricultural facilities and infrastructure, food security, and biosecurity.
        iv. Plantation data
        Data that represents the plantation sector, including bioenergy development and plantation business sustainability
        v. Fishery Data
        The data presented by the fisheries sector includes the empowerment of fishing communities as well as the management of biodiversity and marine conservation.
        vi. State-owned enterprise (SOE) data
        Data representing SOE management.
        vii. Investment data
        Data that provides investment guidance include investment management, investment licensing management, and investment litigation
        viii. Cooperation data
        Data that presents the development of cooperatives include cooperative institutional management, cooperative production and marketing management, cooperative financing empowerment, and cooperative development and cooperative supervision.
        ix. Small and medium business data
        Data that presents the development of small and medium enterprises include institutional management of small and medium enterprises, production

management and marketing of small and medium enterprises, and empowerment of small and medium enterprises financing.

x. Tourism data
Data that represents the tourism sector, including the management of tourism supporting factors and the preparation of a national tourism master plan

3. Infrastructure Data
    a. Regional Development Information
        i. General work data
        Data that represents the field of public works include public works infrastructure management, construction service development, domestic wastewater management, and water resource management.
        ii. Transmigration data
        Data that represents the field of transmigration include education and training on transmigration, research and development of transmigration, and development of transmigration areas.
        iii. Transport data
        Data that represents the field of transportation include management of transportation security and safety, management of transportation services, and management of transportation facilities and infrastructure.
        iv. Housing data Data
        Data that represents the housing sector include management of housing infrastructure, management of the housing environment, development of residential areas, development of strategic facilities and infrastructure, and implementation of housing.
        v. Regional development data or underdeveloped areas
        Data that represents the development of underdeveloped areas or areas include development of underdeveloped areas, development of villages and rural areas, empowerment of rural communities, and development of certain areas.
    b. Environmental and Natural Resources Information
        i. Mining data
        Data that represents the mining sector
        ii. Energy data
        Data representing the energy sector includes electricity and energy conservation.
        iii. Forestry data
        Data that represents the forestry sector include increasing the carrying capacity of watersheds and protected forests as well as protecting forest areas.
        iv. Marine data
        Data that represents the marine sector include maritime management, marine spatial planning, empowerment of marine communities, and management of marine resources.
        v. Environmental data
        Data that represents the environmental field, including climate and weather management and management of climate and weather facilities and infrastructure.
4. Social Services Data
    a. Social Protection and Health Information

i. Health data
Data that represents the health sector include pharmaceuticals and medical devices, P4GN, disease prevention and control, and drug and food control.
ii. Social data
Data that represents the social sector include search and rescue management, human development, handling the poor, and disaster management.
iii. Women empowerment data
Data that presents the fields of women's empowerment include gender equality, child protection, protection of women's rights, and management of child growth and development.
iv. Health data
Data representing the health sector includes pharmaceuticals and medical devices, disease prevention and control, and drug and food control.

b. Public Order and Safety Information
i. Legal data
Data that represents the legal field, including correctional management and immigration administration.
ii. Security data
Data that represents the security sector include security management, order management, transnational countermeasures and terrorism, law enforcement, community protection, and maintaining public peace.
iii. Human rights data
Data that represents the field of human rights including intellectual property rights.

c. Education and Labor Information
i. Education data
Data that represents the field of education includes the development of librarianship and management of education personnel.
ii. Employment data
Data that represents the field of employment include the management of Indonesian migrant workers and the development of occupational safety and health.
iii. Science data
Data that represents the field of science include basic science research, focused inter and multi-disciplinary research, specific sector scientific research, and coordinating the national system of science.
iv. Technology data
Data that presents the technology sector include management of inventions and innovations, remote sensing management, management of aviation and space technology, management of nuclear power, management of technology assessment and application, and coordination of national technology systems.
v. Youth data
Data that presents the field of youth empowerment and development.

d. Cultural and religious information
i. Religious data

Data that represents the field of religion include religious community guidance, religious education and religious training.

ii. Cultural data
Data that represents the field of culture include the development of the national archives, and the development of the national film.

iii. Sports data
Data that represents the field of sports.

5. General Data
    a. General Supporting Data
        i. Government policy
        Data that presents information related to government policies
        ii. Activity Management Data
        Data that presents information related to activities.
        iii. Regional Data
        Data that represents regional information.
        iv. Other Support Data
        Data that represents information not covered by other definitions.

Annex A5 - GGEA v.2.0 Technical Reference Model

1 Overview

Document Purpose

The purpose of the Technical Reference Model is to describe, document and communicate the infrastructure technologies, infrastructure design considerations, technical standards, and best practices to manage the integration and interoperability of Information and Communication Technology (ICT) resources across all MDAs in the GoG.

Objectives and Benefits of TRM

The TRM provides guidance in the design, development and implementation of ICT infrastructure and systems to improve the efficiency, effectiveness, and interoperability of ICT resources across the Government of Ghana.

When adopted by MDAs, the TRM will bring the following benefits:

(a) Align MDAs ICT projects to central ICT initiatives;
(b) Improve decision making in selection of technologies;
(c) Enhance interoperability across MDAs;
(d) Leverage current ICT investment and assets.

Scope of Technical Reference Model

The TRM describes the infrastructure technologies and their respective technical standards that are grouped into five domains. The TRM, however, does not include IT operations which will be addressed under the Process Management section of the Framework. The five domains are:

1) Data Centre
2) Network
3) Platform
4) Service Integration
5) Service Access

Each domain in the TRM will be structured according to the following sections:

a) Intent
b) Relation to Other Domains
c) Domain Design Principles
d) Technology Categories and Components
e) Architecture Design Considerations
f) Technical Standards and General Standards
g) Best Practices
h) Obsolete Technology.

The Figure below depicts shows the TRM with its five domains with detailed description in the following sections

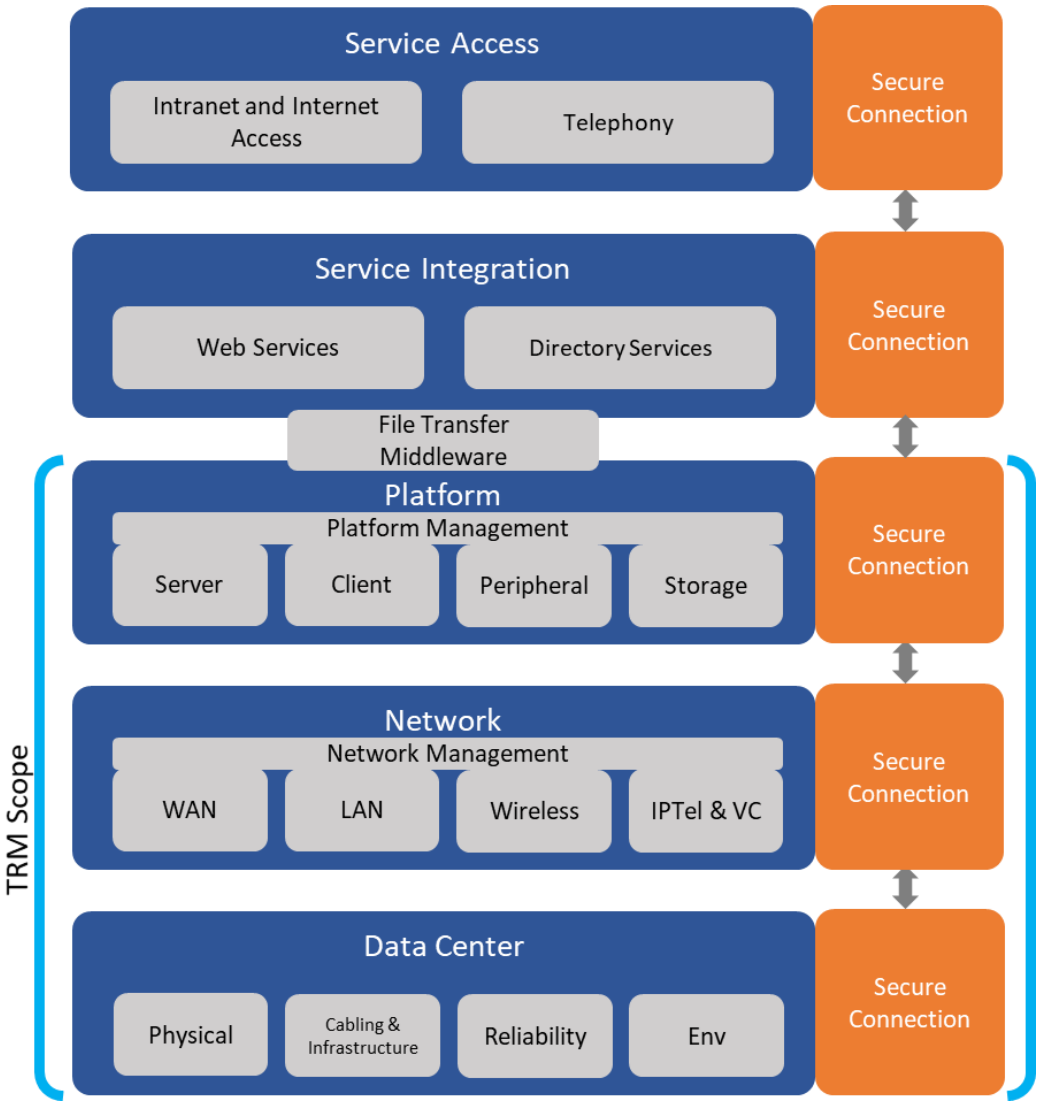

Figure 19 - Technical Reference Model

Relation to Other Ghana Architecture Framework Reference Models

The TRM provides references to the infrastructure technologies and their respective technical standards. and describes the fundamental technology building blocks that are required.

The DRM requires the availability of the infrastructure technologies and technical standards in the TRM to ensure secure and effective data management.

The SRM uses the infrastructure technologies and technical standards defined by TRM to support the development and deployment of applications and electronic services.

The relationship between TRM and BRM is indirect, and is realized via the SRM and IRM. The technologies and standards to automate the lines of business are described in the SRM and IRM.

The Figure below provides a pictorial overview of how the TRM is related to the SRM and IRM.

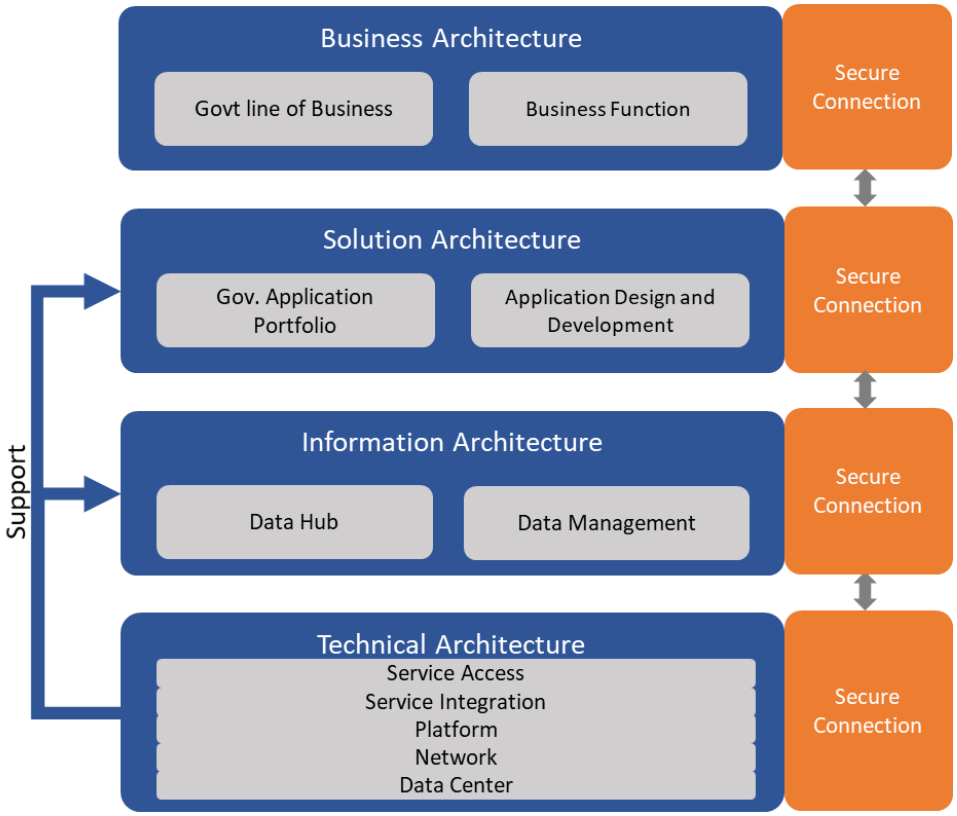

Figure 20 - Relation to Other GGEA v.2.0 Architecture Framework Reference Models

Target Audience

The primary audience of this document is as follows:

a) ICT Managers
The TRM provides insights on central initiatives and the importance of alignment to the Ghana National ICT Plan. It also presents opportunities for management staff such as ICT Directors and Managers to consider consolidation and standardization of the MDAs' infrastructure to manage costs and optimize resources for efficiency.

b) ICT Architects and ICT Planners
ICT architects and planners should use this document when implementing their ICT systems, to leverage on the central initiatives and align with the technical standards.

c) ICT Administrators
By understanding the various infrastructure technologies and central initiatives, government ICT administrators can understand how their roles fit into the overall technical architecture. They can also recommend to the respective MDAs how these technologies can be better administered, shared, and optimized within the MDAs.

d) ICT Vendors
ICT vendors should refer to this document when proposing and implementing ICT projects for MDAs.

Technical Architecture Design Principles

Design principles, which describe the preferred directions, aspired attributes and practices, are required to guide the development of the architecture. The following are the overarching Technical Architecture design principles, while specific design principles for the different technology domains are described in the respective sections:

Principle 1: Optimize and Share Government Infrastructure for Cost- Effectiveness, Operational Efficiency, and Interoperability

ICT infrastructure can be costly to implement and require efficient operations and maintenance. Instead of each MDA implementing its own infrastructure, centralized infrastructure should be the first choice as it promotes sharing and reduces duplication. This optimization would reap benefit on cost effectiveness and operational efficiency with improved government interoperability.

Principle 2: Design Highly Available, Scalable and Adaptive Government Infrastructure

Government infrastructure must support all government services and operations, which includes the various government functions and electronic services to the public (both citizens and businesses). The government infrastructure, thus, must be designed for high availability (round-the-clock), scalability (support growth and voluminous transactions) and adaptability (varied solutions to meet changing business requirements).

Principle 3: Promote Agility and Quality of Government ICT Infrastructure

Agility is the ability to react promptly to changes, while quality refers to the performance and satisfaction derived from using the infrastructure services. These two fundamental attributes ensure government IT infrastructure is built correctly and effectively.

Principle 4: Ensure Security in Development, Implementation and Management of Government Infrastructure

In the development, implementation and management of government infrastructure, security must be taken into serious consideration. Government infrastructure must provide confidentiality, integrity and availability in all aspects of the infrastructure.

Principle 5: Use Open and Vendor-Neutral Standards and Best Practices with Wide Industry Acceptance

The solutions and standards recommended in the Technical Reference Model would have to be practical and easily adopted by the MDAs. The standards and best practices would be open, vendor-neutral and widely accepted in the ICT industry.

Governance of the TRM

The ongoing management and maintenance of the TRM is part of the overall governance of GGEA v.2.0. Ongoing management of the TRM may include reviewing new technologies, technical standards and best practices.

2 Building Government ICT Infrastructure

Intent

The intent of this section is to aid MDAs in planning and building the right ICT infrastructure. The appropriate technologies have to be used in developing ICT infrastructure that supports the implementation of robust applications with secured data exchanges to meet government business requirements.

Need for Agile and Reliable ICT Infrastructure

The Figure below depicts the GGEA v.2.0 Technical Architecture vision.

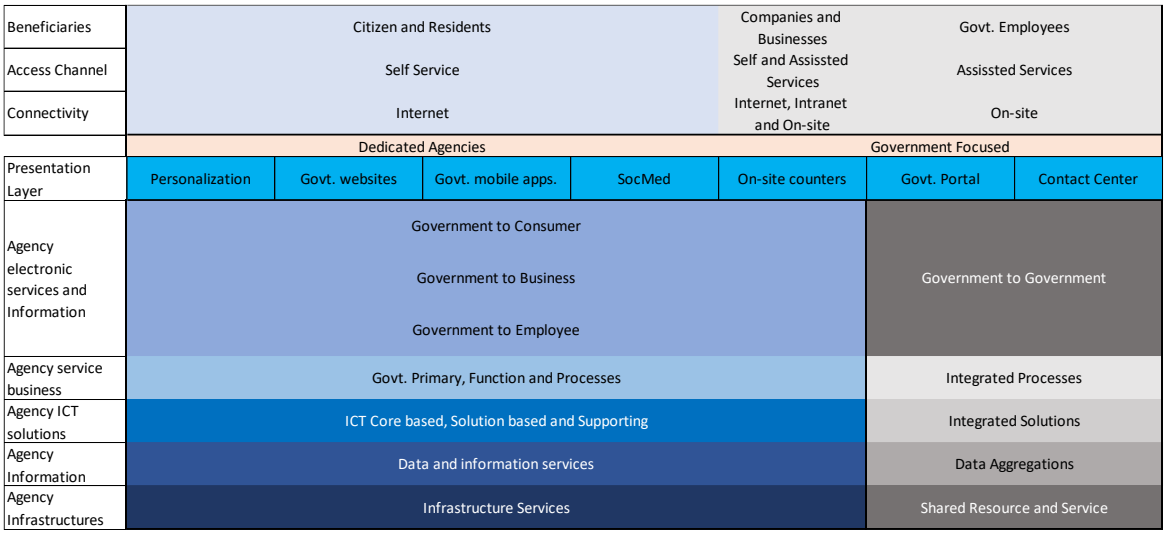

Figure 21 - GGEA v.2.0 Architecture Vision

ICT infrastructure forms the bottom-most layer of the architecture vision. For it to support the layers above it, the ICT infrastructure has to be very reliable. If the ICT infrastructure is not reliable, then the other layers / components such as information and ICT solutions would also be ineffective and not meet business requirements. To meet the dynamic business requirements, the ICT infrastructure also has to be agile to expand its capacity and processing power when required.

While in some cases MDAs may have to build and maintain their own ICT infrastructure, whenever possible they should leverage on shared infrastructure services or central initiatives.

Guide to Implement the Right ICT Infrastructure

The following steps are intended to guide MDAs to implement the right ICT infrastructure:

1) Carry out Infrastructure Capacity Planning

MDA business requirements drive the need for ICT solutions and demands for data / information. In turn, ICT solution and data needs should define ICT capacity requirements in terms of storage size, number of processors, number of users, and sizes of network bandwidth. For future planning, 20% to 30% should be added to initial capacity needs to enable future growth.

2) Assess and Decide on the Best Sourcing Option

Every MDA has primary and enabling government functions (please see Business Reference Model). The provision of ICT is not a primary or an enabling function of MDAs. In short, MDAs have options beyond developing their own infrastructure, including outsourcing ICT infrastructure or other types of ICT provisioning.

The Figure below illustrates the detailed layer of the Ghana Government Technical Infrastructure (i.e., after we zoom in to the infrastructure layer of the Architecture Vision, above).

<table>
<tr><td colspan="6">Agency Focus</td><td colspan="3">Government Focus</td></tr>
<tr><td rowspan="2">Server & Storage Service</td><td rowspan="2">Back-Up & Recovery Service</td><td rowspan="2">Email Service</td><td rowspan="2">Migration Service</td><td rowspan="2">Helpdesk Service</td><td rowspan="2">Monitoring Operations Service</td><td colspan="3">Hosting Service</td></tr>
<tr><td>Digital Certificate Service</td><td></td><td>Technical Security Service</td></tr>
<tr><td colspan="9">Internet Service</td></tr>
<tr><td colspan="9">Agency Network Service</td></tr>
<tr><td colspan="9">Government Network Service</td></tr>
<tr><td></td><td>Data Centre 1</td><td>Computer Room 1</td><td>Computer Room N</td><td>Recovery Centre</td><td></td><td>National Data Center Service</td><td></td><td>DRC Service</td></tr>
</table>

Figure 22 - Infrastructure Layer of the Architecture Vision

Focusing on the right side of the diagram, i.e., government-wide focus, it is recommended that MDAs leverage on these shared infrastructure services and central initiatives. In other words, MDAs should not build and maintain these infrastructures. For details, please refer to ***Shared Services and Central Initiatives.***

For MDA specific infrastructure, MDAs are recommended to consider the following 3 key sourcing options:

i. In-House – build and maintain by the MDA's ICT staff
ii. Outsource – totally outsource the build and maintenance to ICT vendor(s)
iii. Mixed – depending on cost and ability, to build and maintain some ICT infrastructure while outsourcing the others.

Where possible, MDAs are advised to outsource non-critical infrastructure services. Over time, MDAs should outsource as much as they can; taking into consideration factors such as cost and control.

3) Implement and Maintain the Infrastructure

The following are the main infrastructure services that each MDA has to implement and maintain:

a) Physical Infrastructure

The physical infrastructure consists of these components:

Data Centre

A big physical space with the facilities required (power, climate control etc.) to store all the ICT servers, network equipment, cabling infrastructure, etc. Note that a data centre is required only for MDAs that have voluminous ICT capacity and processing requirements. Smaller MDAs should preferably host their applications at the National Data Centre.

or

Server Room

Basically, a server room is a place to store the relevant servers, network equipment and cabling. For smaller MDAs that do not require a data centre but for one reason or another cannot host their applications at the National Data Centre, server room(s) may be sufficient. Typically, an MDA requires a few server rooms at different building locations.

Recovery Centre

Set up like a computer room, but in a separate physical location and used to recover all the ICT applications and data in the event of disaster or other disruptive incident.

MDAs with data centres will require a larger recovery centre (normally, another data centre is used as a back-up or recovery centre). To save costs, MDAs are recommended to use the NDC Recovery Centre Services.

b) Connectivity

To improve communications and operational efficiency, users in different locations of each MDA must be connected digitally. Each MDA must provide network connectivity for its employees through wireless or wired Local Area Networks (LANs). In addition, different branches or buildings of the MDA have to be connected. All MDAs must be connected to the Internet, and all MDAs have to be connected to the Ghana Government Network so that all government employees and services can be accessed.

c) Technical Services

In the past, many ICT projects were implemented with their own set of servers, databases and peripheral equipment. This have resulted in islands of ICT infrastructure that are not fully connected and optimized.

Each MDA is highly recommended to implement technical services instead of simply procuring hardware and software for project implementation. By offering these technical services, different users or business owners within the MDA can request to implement projects where the ICT infrastructure is being optimized with standard quality operational processes. The following technical services are recommended for implementation:

Server and Storage Service

This service is to cater for the demands of the business and solutions in terms of server (or processor) and storage. By delivering this infrastructure as a service, servers and storage can be fully consolidated and optimized so as to reduce cost and improve integration.

Back-Up and Recovery Service

To support business continuity, a back-up service is important to ensure data is correctly backed-up. On a need basis, the back-up data will be used to recover information lost.

Email Service

This is to provide employees in the MDA with access to email and other messaging features.

Migration Service

This service is to ensure proper migration of application codes from test to production. This service can also be extended to the migration of data from test to production and vice-versa.

ICT Helpdesk Service

To provide standard and efficient service to all the employees in the MDA, this helpdesk service allows employees to raise a problem and request help through a telephone call, email or an internal application.

ICT Monitoring and Operations Service

To ensure consistent MDA-wide monitoring of all ICT resources and applications for quality, this service that can be provided for MDA-wide processes.

From a government-wide focus, MDAs are recommended to leverage on currently available technical services such as hosting services (including email), digital certificate and technical security.

3 Data (Computing) Centre Domain

Intent

The Data (Computing) Centre Domain defines the technology categories, technology components and associated standards for physical computing centre. It highlights key architecture design considerations and recommends best practices.

Relation to Other Domains

The Figure below shows the relationship of the Data Centre Domain with the other domains in the Technical Reference Model.

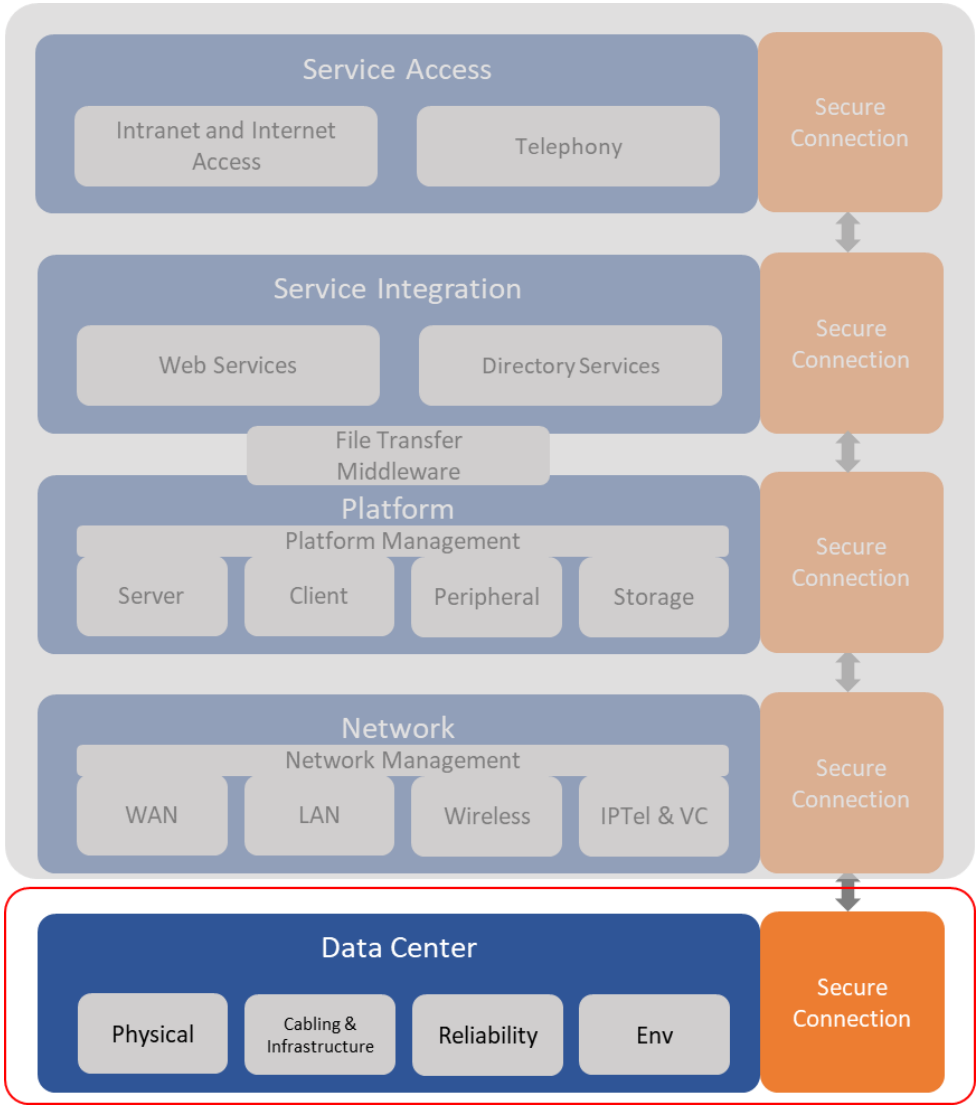

Figure 23 - TRM Data Centre Domain

Domain Design Principles

The following are the Data (Computing) Centre Domain design principles:

Principle 1: Achieve Cost-effectiveness and Operational Efficiency of Computing Centres in Government

The increasing investment in infrastructure dictates that the life span of each additional component or enhancement should maximised to the greatest extent possible. This can be accomplished if the design supports both current needs and anticipated growth potential. Government investments should consider the whole-of- government Total Cost of Ownership (TCO), and overall operational efficiency in maintaining, upgrading and managing government computing centres.

Principle 2: Design Appropriate Government Computing Centres

Depending on the government business requirements, the computing centres must be designed appropriately. For some MDAs, basic availability with simple scalability would be sufficient. For others, robust and high availability computing centres are required to cater for operationally critical business requirements.

Technology Categories and Technology Components

A computing centre can be simply categorized as either a computer room or a data centre. While most of the following technology categories and technology components apply to a computing centre, there are some specific technology components that are applicable only to a data centre.

The Figure below shows the association between the technology categories, technology components and relevant standards.

Figure 24 - Mapping of Categories, Components and Standards for Data Centres Domain

The Table below describes both the technology categories and technology components of the data centre.

Technology Categories	Technology Components
Physical Site Layout This refers to the actual physical site for the data centre.	**Entrance Room** This is the entrance to the computing centre. Typically, there would be only one entrance room to the whole premise for all people.

	Loading Bay This area is where equipment is received and loaded into the computing centre. It has to cater for bulky and heavy equipment.
	Holding Area The area where equipment can be received, checked and unpacked. Typically, suppliers or vendors would deposit the supplies in this holding area.
	Staging Area This place houses all the hardware equipment for configuration, testing and even acclimatization. In addition, this area is also used for testing and deploying software and applications.
	Media Storage Area This area stores all the media such as physical documentation, tapes, and compact discs (CDs).
	Battery Room This room stores the batteries for the whole data centre.
	This is applicable only for data centres
	UPS Room/Area
	This room or area stores all the Uninterruptible Power Supply (UPS) units.
	Generator Area
	is applicable only for data centres.
	Telecoms Room/Area
	This room stores all the key telecommunications such as Private Automatic Exchange (PABX), leased line terminating points and modem devices.
	Service Corridor A secured area where supporting facilities such as power and air-conditioning can be serviced and monitored.
	This is applicable only for data centres.
	Security Centre This secured area houses all the security functions and systems.
	Operations Room/Area This room or area is where daily operations are conducted such as backup, media movements, printouts, inventory updates and audit logs.
	Command Centre This secured area is used to monitor the infrastructure and operations of the data centre. Network Operations Control (NOC) is another

	common name for Command Centre.
	This is applicable only for data centres.
	Computer / Server Room This secured area houses the racks, servers, and network equipment.
	For a data centre, this area can be further divided into the following: (a) Main Distribution Area (MDA) This is a central area where the main cross-connect is located. In addition, this location houses the core network switches and routers. (b) Horizontal Distribution Area (HDA) This place houses the horizontal cabling. More importantly, the cross- connects are in the HDA. (c) Equipment Distribution Area (EDA) This area begins where the horizontal cabling (above at HDA) is terminated at the EDA's patch panel. (d) Zone Distribution Area (ZDA) The ZDA places the optional inter- connection point between HDA and EDA.
Cabling Infrastructure This category describes the various cabling methods used within the computing centre.	**Backbone Cabling** Within the data centre, the backbone cabling connects the MDA and HDA. Optical fibre is used for backbone cabling.
	Horizontal Cabling The horizontal cabling provides connection among HDA, EDA and ZDA. Copper twisted- pair cables are normally used.
Tiered Reliability The different data centre tiers indicate the various reliability measurements. The level of tiered reliability is based on business or application requirements.	**Computing Centre Tiers** There are four (4) computing centre tiers wherein Tier 1 is the lowest and Tier 4 is the highest in terms of reliability. A Computer (Server) room is considered Tier 1.
Environmental Factors These are important factors that affect the design, build and maintenance of the data centre and adhere to the local authority's Safety and environment rules and regulations	**Power** The current and future power requirements must be forecasted. This describes the various power sources, on-site generators, and UPS.
	Cooling The cooling requirements must be made Known to ensure a consistent, cool temperature is kept in the data centre. Air conditioning, water chillers and even methods of housing servers can lower the energy required to keep server temperature within an optimal range.

Table 2 - Data (Computing) Centre Technology Categories and Components

Architecture Design Considerations

The computing centre must support ICT solutions and operations sufficient to meet business requirements. As mentioned above, a computing centre can simply be a computer room, or a data centre. Depending on the business requirements, an MDA may need several computer rooms, or a data centre, or a combination of a data centre and computer rooms.

A computer room typically houses a small number of servers and network equipment to support a small group of users or a small building. A computer room is usually not scalable and does not provide high availability.

A Data centre is usually purpose-built or outfitted to be secure and available 24 hours x 365 days. It is connected to a network whereby servers are co-located and centrally monitored with pre-scheduled planned data centre facility maintenance. This usually does not disrupt the operations of the servers and the services provided.

Data centres are built to meet business needs and requirements. A requirement study must be conducted to identify the needs of a data centre. This is followed by translating the business requirements into Information Technology requirements such as number of racks, central processing units (CPUs), servers and data storage. These ICT specifications are then translated and forecasted with growth consideration in terms of space, power and cooling requirements. Based on the above Technology Categories and Technology Components, the following describes some of the key design elements.

Note: It is important to first read and implement the recommendations in Section 2 Building the Right ICT Infrastructure. For example, carrying out an ICT Capacity Plan is vital as it could lead to making better management decisions on the choice of infrastructure.

When to Implement a Computer (Server) Room

The following are factors for consideration for implementing a computer room:

(a) To cater for a limited number of users within a certain area or building
(b) To house network equipment (wireless and wired) including cabling infrastructure
(c) To house specific servers and storage that support the implementation of ICT solutions used within the area or building only (i.e., not MDA-wide).

When to Implement a Data Centre

The following are factors for consideration for implementing a data centre:

(a) To meet dynamic, robust and demanding government business requirements; for example, the need to provide multiple electronic services and ICT solutions over 24x7 period

(b) To support the implementation of ICT solutions used by large number of users, which exceeds 2000 (i.e., MDA-wide and even government-wide)
(c) To house a large quantity of ICT equipment (i.e., servers, storage and network devices) where the number of racks exceeds 20.

The following additional factors for consideration apply only to data centres. MDAs are advised to consult NITA before embarking on any data centre project.

Location of Data Centre

Areas of consideration when locating data centre:

(a) Safe from man-made and natural disaster
(b) Separate location from the main business functions
(c) Availability of power and telecommunications services
(d) Size and requirement of the data centre.

Data Centre Physical Layout Design

MDAs may take into consideration the various components as described in the technology components above. Figure TA-8 below shows the layout of a typical data centre.

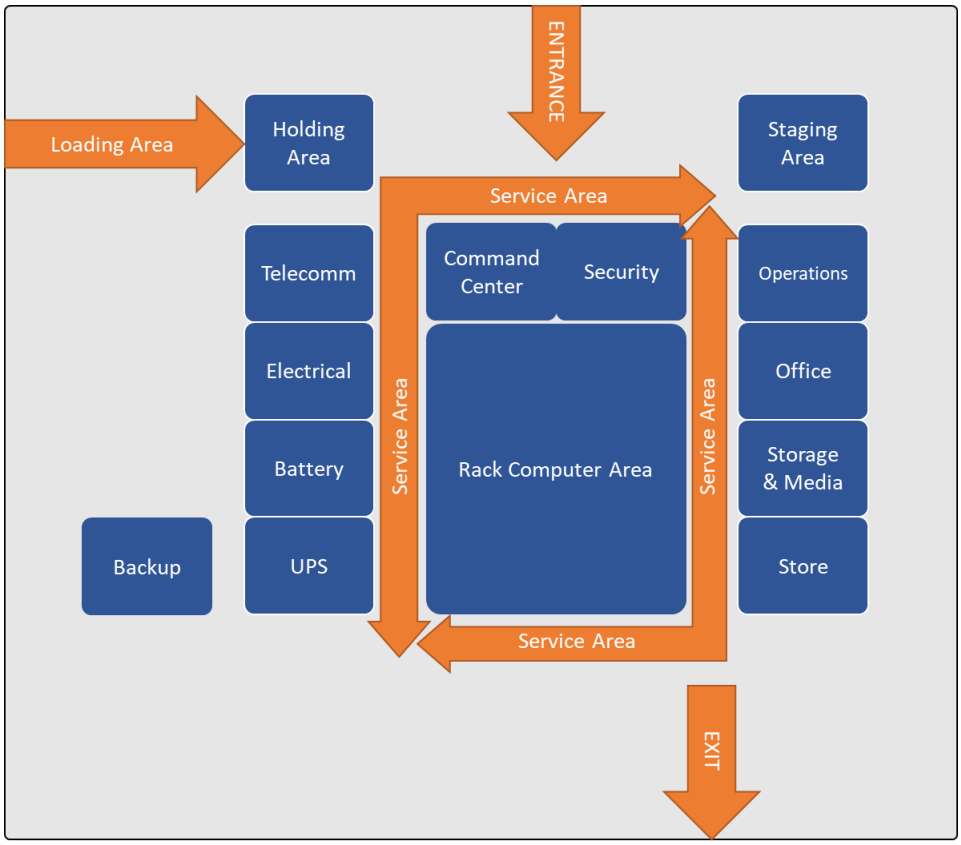

Figure 25 - Sample Data Centre Physical Layout

Tiered Reliability

The TIA-942 Telecommunications Infrastructure Standard for Data Centers published by the Telecommunications Industry Association describes the requirements of the data centre infrastructure as summarized in the Table below. The simplest is a Tier 1 data centre, which is basically a large computer room, following basic guidelines for the installation of computer systems. The most stringent level is a Tier 4 data centre, which is designed to host mission critical computer systems, with fully redundant subsystems and compartmentalized security zones controlled by biometric access controls methods.

Attributes	Tier 1	Tier 2	Tier 3	Tier 4
Building Type		Tenant	Tenant	Standalone
Staffing	None	1 Shift	1+Shifts	"24 By Forever"
Usable For Critical Load	100% N	100% N	90% N	90% N
Initial Gross Watts Per Square Foot (W/ft2)	20-30	40-50	40-60	50-80
Ultimate Gross W/ft2	20-30	40-50	100-150	150+
Uninterruptible Cooling	None	None	Maybe	Yes
Support Space To Raised-Floor Ratio	20%	30%	80%-90%	100+%
Raised-Floor Height (Typical)	12 inches	18 inches	30-36 inches	30-36 inches
Floor Loading lbs/ft2 (Typical)	85	100	150	150
Utility Voltage (Typical)	208, 480	208, 480	12-15 kV	12-15kV
Single Points-of Failure	High susceptible to both planned and unplanned activity	Less susceptible to both planned and unplanned activity	Susceptible to both planned and unplanned activity	Data Center can sustain one case of unplanned event with no load impact
Annual Site-Caused IT Downtime (Actual)	28.8 Hours	22.0 Hours	1.6 Hours	0.4 Hours
Site Availability	99.671%	99.749%	99.982%	99.995%
Months To Implement	3	3-6	15-20	15-20

Table 3 - Tiered Reliability Comparison

Rack Placement

Placement of the racks, in particular the Horizontal Distribution Areas (HDAs), is crucial as it affects the overall power and cooling requirements. To improve cooling efficiency and lower power consumption, the placement of racks should be in a manner to create hot and cold air aisles. Hot and cold aisles ensure general targeted cooling is served to the

equipment. Additional targeted cooling such as in-aisle cooling can be used in cold aisles to augment in areas where required for increased cooling volume such as in rows of racks with high density blade servers. A diagram showing hot-cold aisles arrangement is shown in the Figure below.

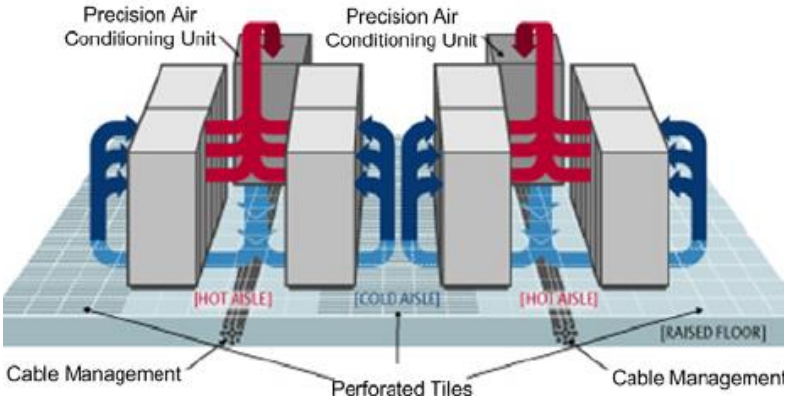

Figure 26 - Creating Hot and Cold Air Aisles

General and Technical Standards

Please refer to the eGIF Technical Standards Compliance List for the general and technical standards for this domain.

Best Practices

Safe Working Environment
As density of data centres has risen with the popularity of blade servers, and in relation to the higher power demand, electro-magnetic field (EMF) interference is factored into TIA 942 standard and also into relevant work place guidelines. This topic should be closely monitored for updated information for a safer data centre working environment in accordance with the update frequency of this document.

Obsolete Technologies

MDAs must ensure that they do not have any obsolete technologies in this domain. Please ensure compliance by referring to Ghana Architecture Framework Obsolete Technologies Compliance List.

4 Network Domain

Intent

The Network Domain defines the network technology categories, technology components and associated standards. It highlights key architecture design considerations and recommends best practices for network implementation.

Relation to Other Domains

The Figure below shows the relationship of the Network Domain with the other domains in the Technical Reference Model.

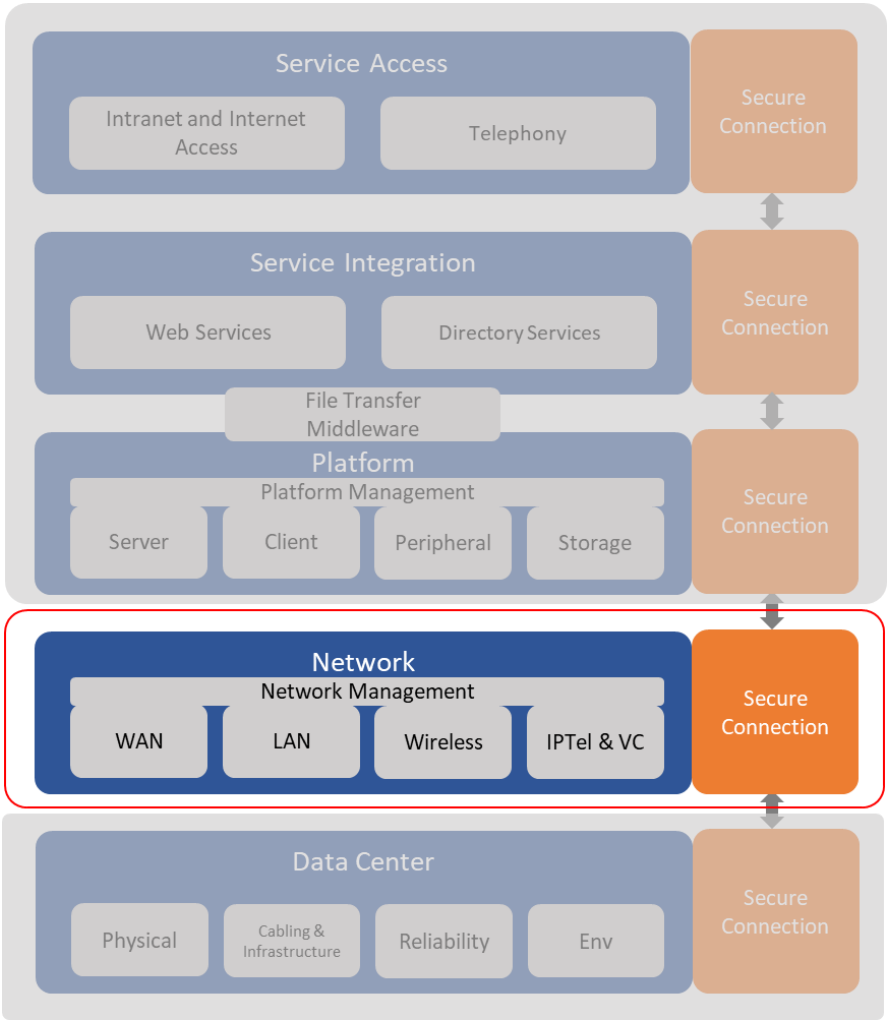

Figure 27 - TRM Network Domain

Domain Design Principles

The following are the four design principles of the Network Domain:

Principle 1: Achieve Cost-effectiveness and Operational Efficiency of Networks in Government

The increasing investment in infrastructure dictates that the life span of each additional component or enhancement should be as long as possible. This can be accomplished if the design supports both current needs and anticipated growth potential. Network investments should consider the Whole-of- Government Total Cost of Ownership (TCO), overall operational efficiency in maintaining, upgrading and managing the Government networks.

Principle 2: Design Highly Available, Scalable and Adaptive Networks

Networks provide an increasingly important and necessary role in the execution of Government business functions and processes. The availability of the network seven days a week and twenty-four hours a day is now a universal requirement.

Networks consist of and rely on many interrelated and often highly complex components distributed across a wide geographic area. Failure of any single component can have severe adverse effects on one or more business applications or services.

Reliable networks contain no single point of failure. Networks are comprised of many components and are often only as reliable as the weakest link. Therefore, reliability and redundancy must be built into the design, not added- on in an ad hoc manner.

Bandwidth must be sufficient and easily scalable to accommodate new and expanding applications, different types of data (e.g., voice, data, image, and video) and a variety of concurrent users.

The government network must be designed to minimize latency and be adaptable to changes in government business needs.

Principle 3: Accommodate Multi-vendor Participation and Support Common, Open, Vendor-neutral Protocols to cater for Interoperability

Open, vendor-neutral protocols provide the flexibility and consistency to allow MDAs to respond more quickly to changing business requirements.

An open, vendor-neutral network allows choosing from a variety of sources and selecting the most economical network solution without impacting applications. This approach supports economic and implementation flexibility because technology components can

be purchased from many vendors, especially those who are widely accepted in the industry. This insulates from unexpected changes in vendor strategies and capabilities.

Principle 4: Design Network for Business Criticality

Network infrastructure should be robust to cope with minimum outages and able to recover quickly. Network infrastructure design should cater for disaster recovery based on the criticality of the business functions. The network design should consider components to support the disaster recovery plans of the ICT system.

Considerations for business-critical requirements, such as low network downtime and faster recovery, results in higher user satisfaction for government electronic services to the public. High network availability is required for continuity of business functions.

Technology Categories and Technology Components

The Figure below shows the association between the Network technology categories, technology components and relevant standards.

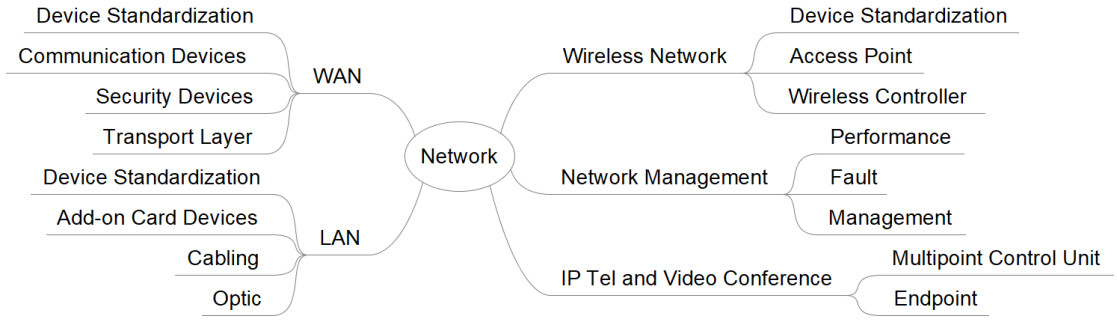

Figure 28 - Mapping of Categories, Components and Standards for Network Domain

The Table following describes both the technology categories and components of the Network Domain.

Technology Categories	Technology Components
Wide Area Network (WAN) This technology category defines communications networks covering multiple distance areas, and may spread across wide geographical areas. WANs often connect multiple smaller networks, such as LANs. The key difference between WAN and LAN technology is scalability. WAN must be able to grow as needed to cover multiple cities, even countries and continents. Typically, a WAN consists of several interconnected routers, and a transmission from any one device is routed to a	**Network Communication Devices** These are hardware and software components which interconnect different sites and locations so that it allows for sharing of resources and information. Examples of network communication devices used in WAN are: a) Routers b) Remote access devices

specified destination device.	
	Security Devices These are the devices deployed with the network communication devices to ensure WAN security: (a) Firewalls (b) Intrusion detection/prevention system
	Transport Layer Method These are types of transport method used for WAN: (a) Point-to-point (b) Circuit switching (c) Packet switching Packet switching (e.g., Multi-Protocol Label Switching) is recommended as the primary WAN transport method due to benefits of scalability and cost- effectiveness.
Local Area Network (LAN) The Local Area Network (LAN) is a data communications infrastructure that is confined to a limited, close-proximity area and involves 2 or more devices that communicate with each other with no external routing.	**Network Communication Devices** These are hardware and software components which interconnect computers so that it allows for sharing of resources and information. Examples of network communication devices are: (a) Edge switch (b) Distribution switch (c) Core switch
	Add-on Card (NIC) This is a computer hardware component designed to allow computers to communicate over a computer network. The NIC is placed in a computer for LAN connectivity, and it is managed by the operating system.
	Cabling System It is a set of cabling and connectivity products that carries voice, data and video. Free Space Optics (FSO) Free Space Optics is used for transmission through the air (between buildings that are in close proximity of 2-4 kilometres) with clear line of sight between the source and the destination, FSO refers to the transmission of modulated visible or infrared (IR) / laser beams through the atmosphere to obtain optical communication.

Wireless Local Area Network (WLAN) Based on LAN, this technology uses radio, microwave or infrared links to replace the physical media of traditional LAN (i.e., wires and cables).	**Wireless Access Point (AP)** This technology component allows wireless communication devices to connect to a wireless network using Wi- Fi, Bluetooth and other wireless technologies.
	Access Controller This component regulates traffic between the open wireless network and important resources. It regulates access to the LAN by authenticating and authorizing users.
	Wireless Network Interface Card Wireless network interface card (wireless NIC) enables users to access the wireless network. It provides the interface between the computer and the antenna.
Internet Protocol (IP) Telephony and Video Conferencing IP Telephony defines a way to carry voice calls over an IP network (such as private enterprise LANs, WANs,intranets and the Internet). Specifically, IP Telephony involves the delivery of the telephony application over IP, instead of circuit-switched or another modality. Video Conferencing supports discussion between 2 or more parties at different locations, where each group can see and hear each other using telecommunication network.	**Multipoint Control Unit** The IP-Telephony Gateway performs the functions of providing call management, interoperability between video/audio and network standards, protocol conversion and audio/video format conversion.
	Endpoint Phone calls are made over the ordinary Public Switched Telephone Network (PSTN). However, IP Phone Client is a device that allows a user to make phone calls over an IP network. Instead of the traditional data, digitized voice is transmitted over the IP network (VoIP). Optional camera on IP phone with higher demand on traffic can enable video call / video conference.
Network Management This technology category defines the technologies to manage, maintain and monitor the various network resources. It allows the discovery, search, and identification, monitoring and even self-healing of network resources situations. As network is crucial in supporting the availability of IT applications and communications, integrated network management is important to ensure an end-to-end delivery of consistent, high- availability network services.	**Fault Management** Fault Management includes the proactive monitoring of network components to detect and resolve problems.
	Performance Monitoring and Management This component defines the network performance (e.g., bandwidth management) and management of the network based on Service Level Agreement (SLA).

Table 4 - Network Technology Categories and Components

Architecture Design Considerations

Wide Area Network (WAN)

A Wide Area Network (WAN) is a communications network covering multiple distance areas and may spread across the wide geographical area. WANs often connect multiple smaller networks, such as Local Area Networks (LANs). WAN must be able to grow as needed to cover multiple cities, even countries and continents. Typically, a WAN consists of several interconnected routers and a transmission from any one device is routed to a specified destination device. It is recommended that all network links be encrypted using cryptographic standards of minimally 128-bit key length for symmetric algorithm or 2048-bit for asymmetric algorithm.

Areas of consideration when implementing WAN:

(a) Router

The router shall support BGP4 (Border Gateway Protocol), OSPF (Open Shortest Path First), PIM (Protocol Independent Multicast) and DVMRP (Distance Vector Multicast Routing Protocol) for efficient routing.

(b) Firewall

Firewall shall be implemented to protect internal network from untrusted network (i.e., Internet). The firewall shall be certified to Common Criteria EAL-4. For high-risk environment, application proxy firewall should be added to stateful packet filtering firewall.

(c) Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ) is usually created at the firewall. It is setup to allow appropriate access to web services for external users while protecting internal network. As DMZ is located between organization's internal network and external network, it is an additional security layer to contain less trusted network traffic.

(d) Intrusion Detection and Prevention System

Network intrusion detection and prevention system should be implemented to inspect network packets and alert in case of intrusion/attacks.

(e) Remote Access / Virtual Private Network (VPN)

Remote access/VPN shall be authenticated using two-factor authentication methods such as token or one-time password and encrypted for data integrity using IPSEC (Internet Protocol Security). Incoming virtual private network (VPN) traffic shall be decrypted just outside the firewall at the VPN gateway, allowing the firewall to perform additional authentication.

Local Area Network (LAN)

The Local Area Network (LAN) is a data communications infrastructure that is confined to a limited, close-proximity area and involves two or more devices that communicate with each other with no external routing.

Areas of consideration when implementing LAN:

LAN is typically designed based on 2-tier or 3-tier network architecture. 2-tier network architecture reduces latency and improves performance. In circumstances where 2-tier is not possible, maximum 3-tier network architecture will be used. Both 2-tier and 3-tier LAN design will deploy Layer 2 and Layer 3 switches. Layer 2 switches are multipoint devices that provide dedicated bandwidth on each port. Layer 3 switches are devices that perform hardware-based routing between Virtual LAN (VLANs) and subnets.

(a) 2-Tier Network Architecture

In 2-tier network architecture, the core switch forms the backbone and an edge switch provides the access to end-devices, as shown in the Figure below.

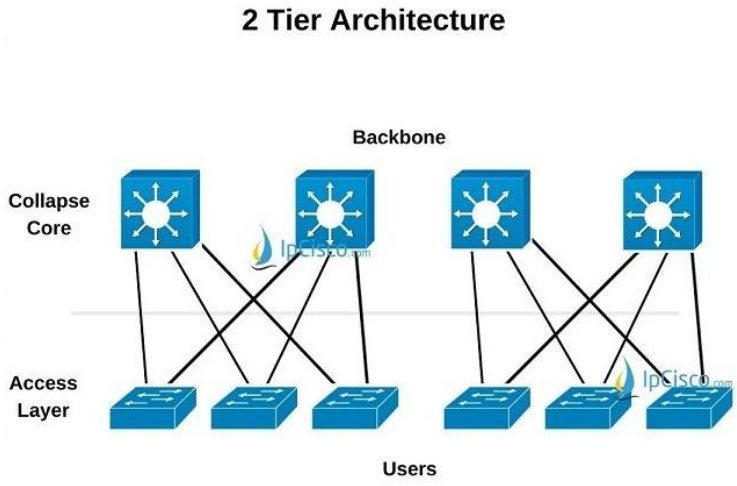

Figure 29 - 2-Tier Network Architecture

(b) 3-Tier Network Architecture

In 3-tier network architecture, the end device will connect to the edge switch. The distribution switch aggregates the traffic coming from the edge switch and forwards it to the Core switch. The Core switch shall be high performance and provide a high level of redundancy within the backplane of switch fabric. Refer to the Figure below.

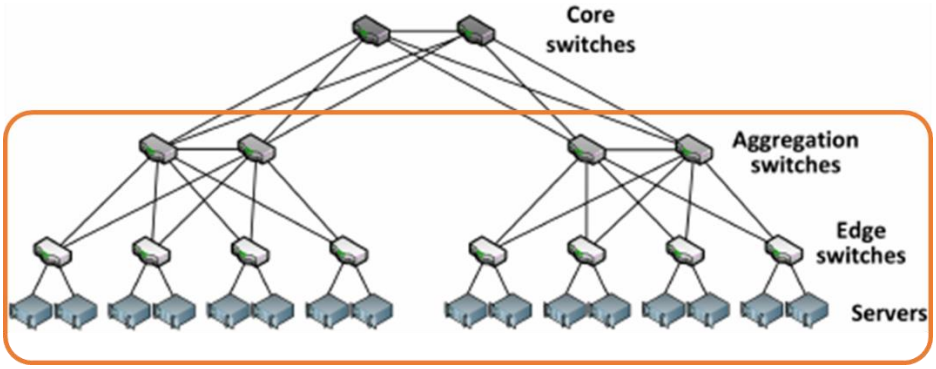

Figure 30 - 3-Tier Network Architecture

(c) Structured Cabling System

As part of a LAN, a Structured Cabling System (SCS) is required to ensure efficient, secured and scalable physical wired connectivity. SCS is the foundation for the whole network infrastructure and therefore MDAs should ensure there are sufficient time and resources so that it is well planned, installed and maintained.

MDAs to consider the following when deploying SCS:

(a) Proper planning to cover all necessary places
(b) Allow for sufficient growth in terms of bandwidth and cable outlets, including outlets for printers, faxes and copiers.
(c) The duration of SCS is normally between ten (10) and fifteen (15) years
(d) Complement with wireless for areas that are physically difficult to lay cables.

Wireless LAN (WLAN)

WLAN is a LAN communication technology in which radio frequency, microwave or infrared links replace physical media (i.e., wires and cables). Radio frequency (RF) is far more popular for its longer-range, higher bandwidth and wider coverage. Most wireless LANs today uses the 2.4-gigahertz (GHz) frequency band also known as Industrial, Scientific and Medical (ISM) bands or 5GHz, Unlicensed National Information Infrastructure (U-NII) band. Using RF technology, it is possible to transmit and receive data over the air, through walls, ceilings and even cement structures, without wired cabling.

Areas of consideration when implementing WLAN:

(a) Coverage: Provides a good network coverage for the envisaged areas
(b) Security: Ensure that the network is not compromised
(c) Manageability: Ability to manage and troubleshoot the wireless network.

IP Telephony

A converged network used to incorporate voice, video and data.

Areas of consideration when implementing IP telephony:

(a) Quality of Service (QoS): Ensure secure, reliable and cost-effective VOIP implementation
(b) Power-over-Ethernet (PoE): Eliminate the need for installation of new AC outlets.

Network Management

Network management tools should be used to manage and troubleshoot network problems.

Areas of consideration when implementing network management:

(a) Fault management: Tools for troubleshooting network problems such as packet analyser and cable tester
(b) Performance monitoring and management: Tools to monitor and collect network statistics such as bandwidth utilization and latency.

General and Technical Standards

Please refer to GGEA v.2.0 Technical Standards Compliance List for the general and technical standards for this domain.

Best Practices

Develop and maintain a set of ICT policies for Computer Network to support ICT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.

The following areas should be covered in the policy:

- Policy on use of network services
- User authentication for external connections
- Equipment identification in networks
- Remote diagnostic and configuration port protection
- Segregation in networks
- Network connection control
- Network routing control

- Network Change Management.

LAN / WLAN

Best practices for LAN/WLAN network implementation include:

a) Groups of information services, users, and information systems should be segregated on networks. To accomplish this segregation at network level IP subnets or VLAN can be used to segregate the network. This is to limit broadcast and improve overall network performance
b) Advance planning and preparation are required to ensure the availability of network services to deliver the required system performance. High availability can be ensured by implementing redundant WAN links, hardware redundancy, fail-over protocol (e.g., VRRP) and redundant links between the edge and core switch.
    - Ensure uplink to the core switch can support at least 20% of the aggregated bandwidth of all the ports of the edge switch.
    - Enable link aggregation to achieve higher bandwidth and load sharing.
    - Enable management agents (e.g., SNMP and RMON) for proactive monitoring to provide alerts on network problems.
    - Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. Use static routing in environments where network traffic is relatively predictable, network design is relatively simple or environments which need higher security. Use dynamic routing in large network environment and when network changes often.
    - Use Layer 3 switch to perform inter-VLAN routing for better performance
    - Disable unnecessary services to prevent abuse by hackers.
    - Implement Wireless LAN as a complementary network to support mobility.
    - Use security techniques and related management procedures (e.g., firewalls, security appliances, intrusion detection) to authorize access and control information flows from and to networks. Security devices should be deployed in a layered defence fashion, concentrating from least trusted network segments (e.g., Internet, DMZ) and also in network with critical resources.
    - LAN should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
    - Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in house or outsourced.
    - Appropriate authentication methods should be used to control access by remote users. Authentication of remote users can be achieved using, for example, PKI,

VPN solutions, using MPLS network for connectivity among government entities and their branches to provide assurance of the source of connections.

Structured Cabling System (SCS)

(a) Special security considerations

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. For highly secured sites, all trunkings must be sealed and tagged with a tamper-proof security tag. The broken seal will indicate that the trunking has been tampered with. Cabling should not be located or run over publicly accessible areas.

The following guidelines for cabling security should be considered:

(i) Power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection.
(ii) network cabling should be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas.
(iii) clearly identifiable cable and equipment markings should be used to minimize handling errors, such as accidental patching of wrong network cables.
(iv) A documented patch list should be used to reduce the possibility of errors.

(b) Future-proof

As an SCS installation is supposed to last for 10-15 years, it may be a long time before a cabling upgrade is forthcoming, while the network technology has far exceeded the performance limits of the current installation. It is therefore important to future-proof the installation. For example, install single mode fibre cables in addition to multi-mode fibre.

(c) Calibration is needed to ensure that the test results are valid

(i) Twisted Pair Cabling Testing
All cables should be individually tested, according to the latest standard of the EIA/TIA 568 and ISO/IEC 11801.The testing methodology should be based on the latest standard of EIA/TIA using a certified cable tester.
(ii) Optical Fibre Cabling Testing
The optical fibres should be tested to the following standards: EIA- 455-171 (FOTP-171) and EIA 526-14. An Optical Time Domain Reflectometer (OTDR) test should be carried out on all new fibres and documented copies of the test results provided. The spectrum to which tests should be carried out should be between 850 nm and 1300 nm for multimode. For single mode, the spectrum to be tested should be between 1310 nm to 1500nm

Both printed and electronic copies of the OTDR traces providing proof of a system's integrity and performance should be obtained. A trace of the entire length of fibre, commonly known as a "signature trace" should be provided.

All fibre optic cables should be tested by power source and light meter prior to installation and again after installation. Power meter test should also be conducted.

(d) Cable routing guidelines

Routing of transmission media should follow the following guidelines:

(i) Cables should be routed to avoid fluorescent light fittings and power cables (exception: optical fibre)
(ii) Power cables should be segregated from communications cables to prevent interference and cables should not be run in the same conduit as power. Crossing power cables is allowed but it must be at right angles, and some form of bridge should be used
(iii) Cables should be routed on trunkings. Cables shall not be tied to ceiling hangars
(iv) Electromagnetic shield should be used to protect the cables
(v) Access should be controlled to patch panels and cable rooms.

(e) Labelling rules

All cable runs should be labelled end-to-end. This includes patch panel, patch cord, station cord, information outlets and main trunking. For fibre, all cable runs must be labelled. Labelling should be followed according to the standard ANSI/TIA-606-B.

(f) Information outlets

Information outlets must be placed at areas away from water to avoid damages and public areas to avoid unauthorized access.

(g) Access length on the horizontal run

For office with raised floors, there must be a slack of three meters allowance for horizontal run to allow for future adjustment of information outlets location provided it does not exceed ninety meters link specification.

Cabling in Site Preparation

(a) Topology

The cabling topology for the Campus Backbone Subsystem should be star, i.e., separate cables from the Network Centre (in the main building) to each of the auxiliary LAN rooms (in the auxiliary buildings).

(b) Structural guidelines

(i) Raised floors should be provided for all network rooms and should be of anti-static High-Pressured Laminate (HPL) type

(ii) The floor of the Network Centre should be raised access system for running cabling underneath, and able to withstand specified vibration levels in the building code. The floor material should be static free. The floor should support a concentrated floor loading of kN/m2.
(iii) The walls and doors of the Network Centre should be made of fire- resistant rated materials. All basement network rooms are to be constructed with scupper drains, gradient of at least 1:100, and waterproofing on all diaphragm walls. All basement network rooms should be installed with moisture sensors under the raised floor.

(c) Environmental guidelines

The selection and design of the layout of a Network Centre should consider the risk associated with natural and man-made disasters, whilst considering relevant laws and regulations, such as occupational health and safety regulations.

Measures for protection against environment factors should be designed and implemented in Network Centre. Install specialized equipment and devices to monitor and control the environment.

Guidelines must be followed to avoid damage from fire, flood, earthquake, and other forms of natural or man-made disaster in the Network Center.

(i) Air conditioning should be provided twenty-four (24) hours. Hence, vapor insulation must be installed in these rooms.
(ii) 40-60 % relative humidity
(iii) Temperatures 18°C to 24°C
(iv) Heat dissipation rate 12,000 to 16,000 BTU/hr per rack
(v) Free from dust and contaminant
(vi) Adequate uniform lighting of at least 540 lux (50 foot-candles) lighting level
(vii) Provide static-free environment
(viii) Emergency lighting and other safety systems must be provided
(ix) Fire-protection system such as FM200 or other system such as Aragonite Gas system and Smoke detection should be provided
(x) Fire prevention mechanisms installed in the network rooms should comply with the code of practice for fire precautions
(xi) Hazardous or combustible materials should be stored at a safe distance from a Network Room. Bulk supplies such as stationery should not be stored within a Network room.

(d) Physical Security guidelines

Physical security measures must be capable of effectively preventing, detecting, and mitigating risks relating to theft, terror, Information disclosure, unauthorized access, etc.

Following guidelines should be considered to prevent unauthorized physical access, damage, and interference to the Network Centre.

(i) Network Centre should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
(ii) Access to Network Centre should be controlled and restricted to authorized persons only; authentication controls, e.g., access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained.
(iii) Third party support service personnel should be granted restricted access to secure areas or sensitive information processing facilities only when required; this access should be authorized and monitored.
(iv) Access rights to secure areas should be regularly reviewed and updated and revoked when necessary.

(e) Power guidelines

Continuous power must be supplied to the network equipment in the Network Center. In the event of main power failure, this can be in the form of backup power generators and/or UPS.

The power requirements of all possible equipment in the Network Centre must be considered to prevent overloading. In general, more power loops must be supplied in the Network Centre because of the.higher power consumption of the network equipment. There must be at least two separate power sources to the Network Centre, one preferably connected to a source with automatic fail-over backup power supply. Both 13 A and 15 A power outlets should be provided.

Temporary power supplies should not be used for testing servers and network equipment.

(f) Placement and accessibility guidelines

The placement of the Network Centre should avoid locations that restrict or limit expansion. If there is no space for expansion, the establishment of an additional Network Centre will be very costly because of the re- wiring and the base space requirements.

The Network Centre must be centrally located to minimize the length of the cable runs. It must also be accessible to all cable pathways.

The location of the Network Centre must be free and away from water and steam infiltration, humidity, heat, boiler rooms, washrooms, janitor's Rooms. Since the equipment is sensitive to EMI, it must be away from sources of EMI (e.g., transformers, power generators, antennas, lift motor rooms etc.).

The Network Centre should contain no combustible materials, and it should not be used as storage rooms.

(g) LAN Room Subsystem

The LAN Room is the distribution point (fan-out) from the Building Backbone Subsystem to the Horizontal Subsystem. The LAN Room is floor-serving, as opposed to building-serving Network Centre.

(h) Minimize the Number of LAN Rooms

It is not mandatory to have a LAN Room at each floor of the building. The same LAN Room can serve multiple floors as long as the 90 m limit for the Horizontal Subsystem is met. Cable run from LAN Rooms to the Network Centre should take separate route for redundancy, if deemed critical.

(i) LAN Riser Design and Placement

All LAN Rooms should preferably be vertically aligned and situated next to the LAN riser to provide the shortest path between floors. The LAN riser for the LAN Room should be a separate riser apart from telecommunications and power risers. The separation is to prevent physical and EM interference, plus the ease of maintenance and troubleshooting. The LAN riser must be dedicated for SCS installation only. No cable services should share the same void as a lightning conductor or lift shaft.

The riser must be fire stopped at every floor. Firestopping material must be applied to the remaining gap at every floor to seal it. Racks in the LAN Room should dissipate a maximum of 7,500 BTU/hr per rack.

(j) Security Guidelines for LAN Rooms

The LAN Rooms are restricted areas; it must be secured with limited personnel access.

(k) Sizing Racks

Each equipment rack housing both data and voice patch panels should be able to support 144 to 192 points (72 to 96 network data connections and 72 to 96 voice points).

(l) Weight/loading

Each fully loaded rack (with equipment) can have a maximum weight of 480 kg (on 1m2 of flooring). Hence the floor must be able to sustain this weight.

(m) Capacity Planning

The numbers of strands of fibre needed are highly dependent on the current needs of the facility. As a rule of thumb, for each connection between two points, there should be at least 50% spare capacity based on the requirements at time of installation. In addition, cater for an additional 25% spare capacity on single mode fibres on the total fibre requirements at time of installation.

(n) Additional Installation Procedures for SCS

The cable run must be continuous from end to end; splices are not permitted anywhere in the cable run except at the termination points in the Fibre Optic patch panel. An exception is when the cable run is more than 500 m and exceeding the length of a cable drum. All cable runs must terminate in a Fibre Optic patch panel on both ends. All cable runs

outdoors must be run in the external conduit. The external conduit must be tough and made of corrosion-resistant material such as concrete encased uPVC.

Sufficient slack should be maintained at the Network Centre, in case re-termination/adjustment is needed. At least 5 m of slack cable (including the insulation jacket) in each Network Centre must be maintained.

Sufficient slack should be maintained at the LAN Rooms, in case re-termination/adjustment is needed. At least three (3) m of slack cable (including the insulation jacket) in each end must be maintained.

(o) Raised Access Floor System

The cables should run in the space below the raised floor, in rigid pathways such as metallic trunking or conduits.

(p) False Ceiling System

The cables should run in the space above the false ceiling in rigid pathways such as metallic trunking or conduits.

(q) Building power supply

Two separate power loops should be provided in the Network Centres and LAN Rooms. Public power supply and emergency power supply with backup power generator with automatic fail-over in case the public power supply fails. The difference should be clearly labelled on the power socket.

(r) ELCB

Power supply for computer and network equipment should use an ELCB (earth leakage circuit breaker) with a rating of 100 mA to avoid unnecessary tripping.

(s) Grounding

A clean ground, apart from the power ground, must be provided for grounding telecommunication and network equipment.

The entire clean grounding system should meet the ground potential difference limits of 1V R.M.S., and a low resistance between two grounds on the network. This path is measured from the induced point to the ground electrode.

(t) Ground Electrode and Conductor

All grounding electrodes in the building should be bonded together to reduce the effects of differences in ground potential.

Ground conductors are attached to the grounding electrodes to every Network Centre and LAN Rooms. The ground conductors should be earth wires with a solid copper core of at least 6 AWG in diameter. It is recommended that metallic conduits used to house ground conductors and should be bonded to the ground conductor at both ends.

(u) Grounding Bar

At each Network Centre and LAN Room, the ground conductors should be terminated on wall-mounted grounding bar.

(v) Grounding of Equipment Mounting and Components

Each equipment mounting should attach to the grounding bar using 6 AWG earth wires. The path to ground must be permanent and continuous. It is recommended that each equipment mounting be individually bonded, to assure the continuity of the ground path.

Condition	Minimum separation distance		
	< 2 kVA	2 – 5 kVA	> 5 kVA
Unshielded power lines or electrical equipment in proximity to open or non-metal pathways for telecommunication cables	127 mm	305 mm	610 mm
Unshielded power lines or electrical equipment in proximity to a grounded metallic pathway for telecommunication cables	64 mm	152 mm	305 mm
Power lines enclosed in a grounded metallic pathway in proximity to a grounded metallic pathway for telecommunication cables	-	76 mm	152 mm

Table 5 - Separation of Telecommunications Pathways (Source: ANSI/EIA/TIA 569-A)

(w) Water-free area

All Network Centre and LAN Rooms should not be situated next to water facilities (e.g., toilets and wash areas). If this cannot be avoided, the following precautions should be taken:

(i) A kerb of at least 100mm higher than the raised floor should be constructed at the wall dividing the wet area and LAN Room
(ii) Waterproofing must be applied on both sides of the wall separating the wet area and LAN Room
(iii) Waterproofing warranty should last for at least ten years
(iv) A 24-hour bonding test must be carried out and witnessed by the user
(v) Waterproofing coat must be at least 1.5mm thick
(vi) Moisture sensor to be installed under the raised floor of the affected LAN Room.

Obsolete Technologies

MDAs must ensure that they do not have any obsolete technologies in this domain. Please ensure compliance by referring to eGIF v.2.0 Obsolete Technologies Compliance List Platform Domain.

5 Platform Domain

Intent

The Platform Domain defines the technology categories, technology components and associated standards of technical computing devices and peripherals. It highlights key architecture design considerations and recommends best practices for platform implementation.

Relation to Other Domains

The Figure below shows the relationship of Platform Domain with the other domains in the Technical Reference Model.

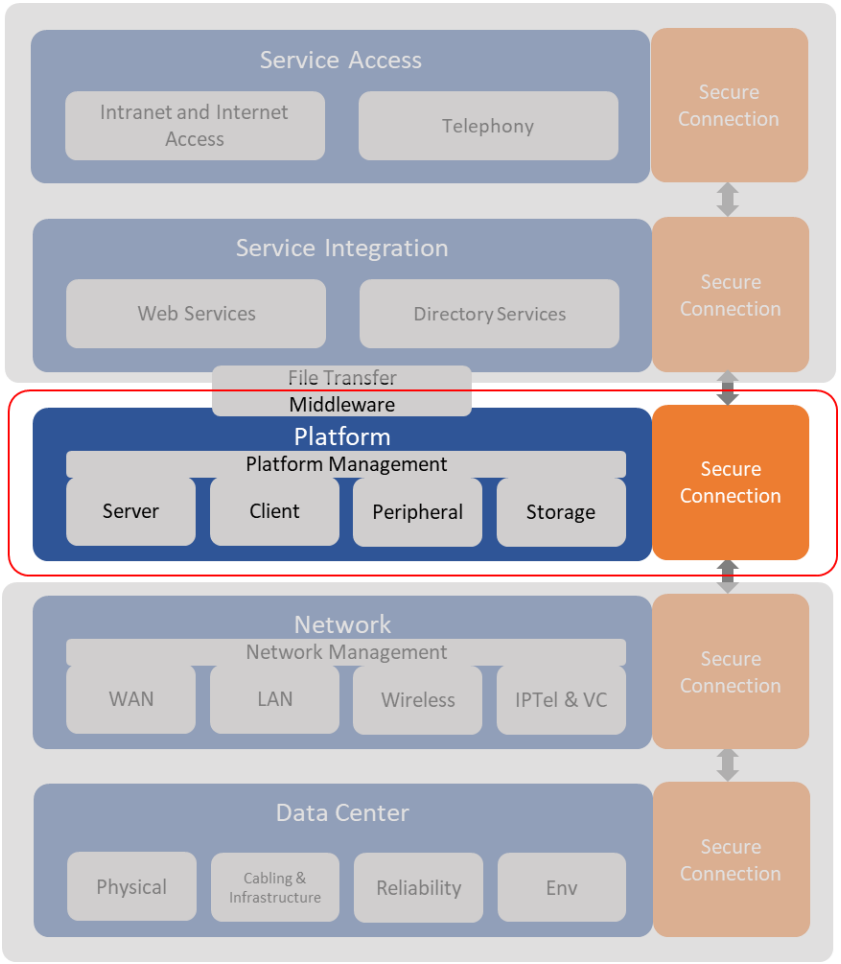

Figure 31 - TRM Platform Domain

Domain Design Principles

The following are the Platform Domain design principles.

Principle 1: Design Mission Critical or Important Systems that Provide Reliability, Availability and Serviceability (RAS)

With RAS, there will be smooth government business operations which avoid loss of data, time and customer confidence caused by system failures. Systems should be designed to permit continued operations, albeit at reduced throughput, even when a physical component fails in normal operations or in the event of a disaster. With the right design and implementation strategy, distributed systems can be extremely robust.

Principle 2: Support Industry-wide, Open, Vendor-neutral Standards to Cater for System Interoperability

Open, vendor-neutral system standards provide flexibility and consistency that will allow MDAs to respond more quickly in an environment of changing business requirements. Vendor-neutral systems support economic and implementation flexibility, and protect against unexpected changes in vendor strategies and capabilities.

Principle 3: Long-term Business Needs are Key Factors in the Choice of Platforms

When selecting a platform for applications to support current business needs, it is worthwhile to ensure the robustness and scalability of the platform to support future growth and change in the technology landscape. The right platform that care for future needs will allow continuous operations when there is a change of business and operation requirements.

Cooperative efforts among MDAs to leverage on shared platform, where applicable, may provide a more cost-effective solution. File and print servers, for example, can be implemented as shared resources among the MDAs.

Technology Categories and Technology Standards

The Figure below shows the association between the technology categories, technology components and its relevant standards.

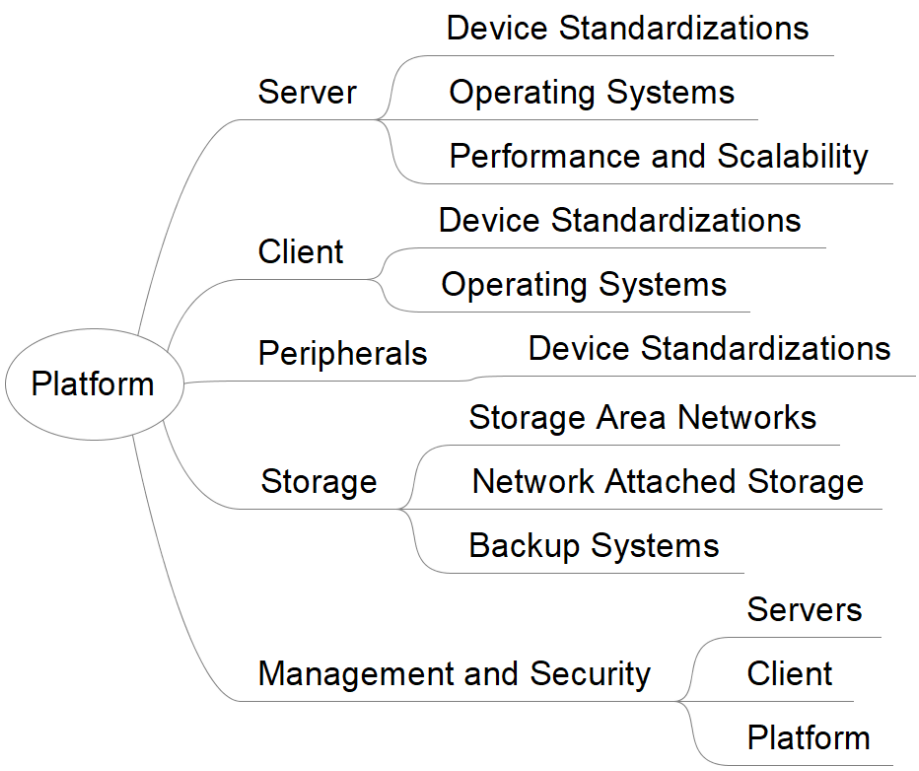

Figure 32 - Mapping of Categories, Components and Standards for Platform Domain

The Table below describes both the technology categories and components of the Platform Domain.

Technology Categories	Technology Components
Servers Servers are powerful computer that consist of multiple processors, memory modules and large disk storage. They are usually used for processing backend applications that are shared by a large number of end users.	**Processor** This is the core technology that processes the millions of computing instructions within a second. A server typically has 2 or more processors. Alternatively, it can also be a dual-core processor where 2 processors are grouped as 1 processor.
	Operating System (OS) This is a software component that is responsible for the management and coordination of system activities and the sharing of the server resources.
	Random Access Memory (RAM) This component defines the memory of the system in the server on a temporary (cache memory) or permanent basis.

	Hard Disk (HDD) This component stores the data or programmes in the server on a temporary or permanent basis.
	Load Balancer This component delivers horizontal server scalability by distributing processing requests among a group of servers based on the nature of the request and the availability of the servers. The load balancer should support the following load balancing methods: **(a)** Random Allocation **(b)** Round robin **(c)** Weighted round robin **(d)** Least connections **(e)** Weighted Least connections **(f)** Response time
Clients Client is a personal computing platform on which application services of interest to the individuals can be performed selectively, as and when required by the individual.	**Processor** This component processes the millions of computing instructions within a second. A client typically has 1 processor or 1 dual-core processor.
	Operating System (OS) This is a software component that is responsible for the management and coordination of system activities and the sharing of the computing resources. Unlike Server OS, there is a wider range of OS that supports multiple processor technologies.
	Random Access Memory (RAM) This component defines the memory of the system in the client on a temporary (cache memory) or permanent basis.
	Hard Disk (HDD) This component stores the data or programmes in the client on a temporary or permanent basis.
Peripherals Devices that extend the client / server capability.	**Peripheral Devices** These devices enable administrative activities in an office environment such as scanning, printing, faxing and photocopying to be carried out efficiently.
Storage and Backup Hardware where data is kept for access by clients and servers. Copies of data are made and stored separately for data recovery.	**Storage Area Network (SAN)** It is a dedicated network that connects Multiple heterogeneous servers to a common pool of storage devices. It has the following benefits: (a) High scalability (b) Transparent scalability (c) Supports LAN-free backup (d) Sharable storage (e) Reusable storage

	(f) Richer storage functionalities including snapshot, local and remote mirroring Robust storage architecture.
	Networked Attached Storage (NAS) It is essentially a special purpose networked file server that supports both the Network File System (NFS) and Common Internet File System (CIFS) file systems. It is less efficient than a SAN in terms of network performance, but it does have benefits similar to a SAN: (a) High scalability (b) Transparent scalability (c) Sharable storage (d) Reusable storage (e) Richer storage functionalities including snapshot, local and remote mirroring (f) Robust storage architecture.
	Backup system The backup system and software are components that provide reliable data backup and restoration.
Platform Management and Security Management tools that allow system administration and monitoring. This category also describes the platform security technologies.	**Server Management** This component defines the management of heterogeneous servers.
	Client Management This component defines the management of clients in a distributed environment.
	Storage and Backup Management This component defines the storage and backup management in a distributed environment.
	Platform Security This component defines the key platform security technologies.

Table 6 - Platform Technology Categories and Components

Architecture Design Considerations

Server

A server is a device that allows multiple users to access network services simultaneously. Servers consists of multiple processors, memory modules and large disk storage. They are usually used for processing of backend applications that are shared by many end users, through their personal computers, portable computers or personal digital assistants connected to the servers through a wired or wireless network.

Areas of Consideration When Selecting Servers:

(a) High-end servers

High-end servers are highly scalable, high available servers designed for mission critical network computing. These servers are usually required for very high processing power such as real-time transactional processing or mission-critical systems.

(b) Mid-range servers

Mid-range servers are positioned between department level and government-wide server solutions and designed to deliver high performance to protect ICT investments over time. These servers are normally used for enterprise-wide solutions (e.g., Enterprise Resource Planning System, Customer Relationship Management System and Database Management System).

(c) Entry-level servers

Entry-level servers are less powerful servers that support departmental or workgroup-level applications. These servers are designed for general purpose use and cost/performance optimization and are scalable and reliable. They can range from single processor systems to quad (four) processors running on multiple operating systems. These servers are suitable for general infrastructure services such as file print, Domain Naming Services (DNS), and small departmental applications.

To achieve high reliability, availability and serviceability, the server should be modular and support the following features:

(i) Support ECC (Error correction code) protection for memory
(ii) Support minimum 2 internal hard disks
(iii) Support dual network interface cards
(iv) Support N+1 hot plug power supply and fan
(v) Support Simple Network Management Protocol (SNMP) and light- out management feature
(vi) Support easy component upgrade/replacement without disrupting on-going system operations.

(d) Server form factors

The Table below describes the different form factors of servers.

Server Form	Description
Tower	A server built in an upright cabinet that stands alone. The cabinet, called a tower, is similar in size and shape to the cabinet for a tower- style personal computer. The tower server is not designed to be rack mounted.

Rack-Optimized	A dedicated server designed to be installed in a framework called a rack. The rack contains multiple mounting slots called bays, each designed to hold a hardware unit secured in place with screws. A rack server has a low-profile enclosure, in contrast to a tower server, which is built into an upright, standalone tower.
Blade	Small form factor servers designed for high density. Usually house in a blade enclosure, which can hold multiple blade servers. The enclosure provides services such as power, cooling, networking, various interconnects and management. Together these form a blade system.

Table 7 - Server Form Factors

(e) Server minimum configuration

The recommended minimum configurations for Explicitly Parallel Instruction Computing (EPIC) / Reduced Instruction Set Computer (RISC) and x86 platforms are shown in Table TA-7.

	EPIC/RISC		x86	
	CPU (single or multi-core)	RAM (GB)	CPU (multi-core)	RAM (GB)
High-end server	8	64	4	32
Mid-range server	4	32	2	16
Entry-level server	1	4	1	4

Table 8 - Recommended Minimum Server Configurations

The recommended minimum configurations will be used as a guide, and it may vary depending on the actual requirements of the applications.

(f) Load balancer

Hardware or software load balancer can be deployed to deliver horizontal server scalability. Hardware load balancer generally provides better performance and manageability. The load balancer should support the following load balancing methods:

(i) Random allocation
(ii) Round robin
(iii) Weighted round robin
(iv) Least connections
(v) Weighted least connections
(vi) Response time.

Clients

A Client is a personal computing platform on which application services of interest to individuals can be performed selectively, as and when required by the individual. It consists of processor, operating system, random access memory (RAM) and hard disk.

Areas of consideration when selecting client device:

(a) Desktop computers

A desktop computer is a computer that is designed for regular use within a personal workspace and offers access to applications and office productivity tools. Desktops should be offered to deskbound and task- based officer (e.g., counter service officer).

(b) Portable computers

A portable computer is designed to be easily carried by hand from one place to another. Portable computer is also commonly referred to as notebook. Portable computers should be offered to non-deskbound officer who require access to information and corporate resources within and outside the office (e.g., knowledge worker).

(c) Personal Digital Assistant (PDA)

A PDA is small mobile hand-held device for personal use that can store and retrieve information. PDA should be offered as an option in addition to desktops or portable computers depending on job requirement (e.g., officer issuing parking fine using a PDA).

The recommended minimum configurations for Clients are shown in Table TA-8.

Type of Client	Recommendation
Desktop computer and portable computer	Latest processor technology
	Minimum 2GB RAM and 160GB hard disk
	Clock speed (depending on mainstream or entry)
Personal Digital Assistant	128MB RAM
	Wireless (Wi-Fi) and Bluetooth enabled
	Mobile phone function with GPRS enabled

Table 9 - Recommended Minimum Client Configuration

Peripherals

Areas of consideration when selecting peripherals:

Use network-attached Multi-Functional Peripherals (MFP) to provide print (duplex capability), scanner, photocopy, and fax features.

Storage and Backup

Areas of consideration when selecting storage and backup

(a) Use SAN instead of storage at server level to achieve the following benefits:
  (i) Redundant data paths and drive connections
  (ii) Dual fiber channel switches and storage controllers
  (iii) Battery backup and redundant power supplies
  (iv) Hot swappable fiber channel disk drives
  (v) Multiple vendor operating system environment support
  (vi) Support RAID configurations
    - RAID 0 (Striping)
    - RAID 1 (Mirroring)
    - RAID 5 (Striping with distributed parity)
    - RAID 6 (Striping with a set of distributed parity)
    - RAID 10 (Stripping of mirrored array).

The figure below illustrates an indicative SAN design.

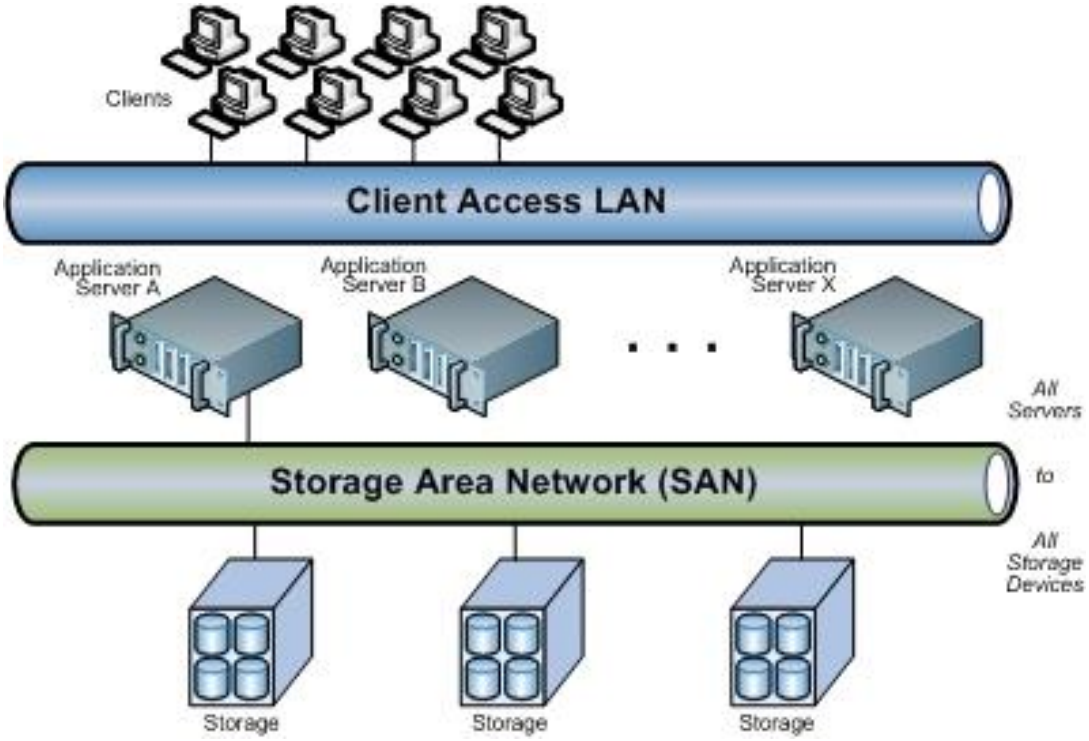

Figure 33 – Indicative SAN Design

(b) Use LAN-free backup for data backup to a shared, central storage device without sending over the local area network.
   (i) Support Linear Tape Open (LTO) and Super Digital Linear Tape (SDLT) technology
   (ii) Support multi-cartridges with autoloader
   (iii) Support various backup methods including full, increment and snapshot.

(c) Use Reference Information Storage System (RISS) and Content Addressed Storage (CAS) to provide index and search capabilities for reference information.

General and Technical Standards

Please refer to GGEA v.2.0 Technical Standards Compliance List for the general and technical standards for this domain.

Best Practices

(a) Take peak load into consideration while planning server capacity
(b) Use server clustering and/or load balancing to achieve higher availability
(c) Segregate development, test and production servers for security
(d) Use KVM switch to manage multiple servers with one common set of console to optimize space utilization
(e) Use Un-interruptible Power Supply (UPS) for servers
(f) Use hardware load balancer instead of software load balancer for better performance
(g) Use SAN for disk storage consolidation
(h) Implement security zoning to increase security protection of a SAN that is shared across different network segments
(i) Configure SAN management interface on a separate physical LAN for SAN management
(j) Replicate mission-critical data on real-time basis across WAN between two storage systems for disaster recovery
(k) Implement autoloader backup system for unattended backup requirements
(l) Implement point-in-time snapshot to backup large database to achieve higher database uptime
(m) Implement full system backup over incremental backup for faster data recovery if required. Generally full system backup should be implemented on weekly basis with incremental backup recommended for daily basis
(n) Test backup media restoration regularly to ensure data recoverability
(o) Store latest backup tapes off-site for disaster recovery
(p) Continuously captures or tracks data modifications and store changes independent of the primary data
(q) Use data de-duplication to reduce disk capacity requirements for recurring backup operations

(r) Encrypt the hard disk of portable computer when used to store confidential data
(s) Consider physical size, weight and battery life for portable computer selection
(t) Use Hardware Security Module (HSM) for storing security credentials (e.g., encryption keys)
(u) Consider different security profiles for client devices depending on the level of risk. Security considerations for profiles may include strong authentication, fully lock down, layer protection (i.e., BIOS) and data protection (e.g., hard disk encryption, file-level encryption).

Obsolete Technologies

MDAs must ensure that they do not have any obsolete technologies in this domain.

Annex A6 - GGEA v.2.0 Security Reference Model (ScRM)

Overview

The purpose of security is to protect and secure the Government's information resources in order to provide an environment in which the Ghana's e-Government business can be safely transacted. Protecting the information and systems that the Government depends on is important as MDAs increasingly rely on new technology.

The term "information security" means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide:

1. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
2. Confidentiality, which means preserving authorised restrictions from access and disclosure, including means for protecting personal privacy and proprietary information;
3. Availability, which means ensuring timely and reliable access to and use of information.

The purpose of the Security Reference Model is to describe, document and communicate the infrastructure technologies, infrastructure design consideration, technical standards, and best practices to manage the integration and interoperability of Information and Communication Technology (ICT) resources across all government agencies in the Government of Ghana.

Objectives and Benefits of ScRM

Security architecture is a framework that describes the function, structure and interrelationships of the security components within an environment. Security architecture consists of layers of policy, standards and procedures and further describes the way these elements are linked to create an environment in which security controls can be easily established within the context of a large complex organization.

To meet the needs of enterprise-scale security, the proposed security architecture provides the basic framework for approaching security while maintaining consistency across MDAs. The main objectives of the Security Architecture are to:

- Define the security dimensions;

- Focus security efforts to ensure the proper controls are implemented to adequately protect information assets based on strategic drivers;
- Create a structure around security to integrate it into the overall business context; and
- Provide a prioritised road map for work units to progress towards this overall model.

The benefits of developing and implementing security architecture include a business-driven, enterprise approach to security services and architecture through the development of enterprise rather than point solutions. Other efficiencies include reduced costs, improved risk management and the enablement of key government objectives. A security architecture provides increased agility when responding to changing needs, and a structured, Government-wide approach to manage information security.

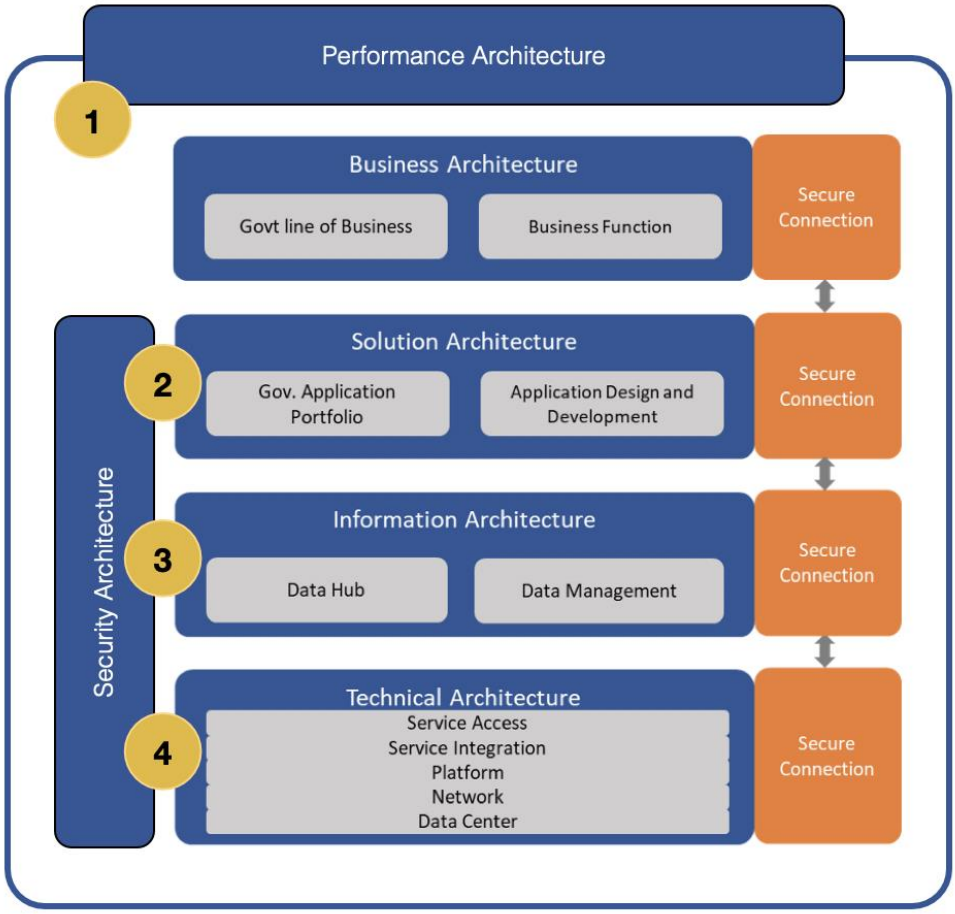

Figure 34 - Relationship Between Security and other Architecture Domains

Role of Security Architecture Relative to Other Architecture Domains

The Security Architecture described in this section is an integral part of Ghana's overall Government Enterprise Architecture and has a cause-and-effect relationshio witheach of the other Architecture Domains. The numbered circles in the Figure above indicate how Security Architecture interacts with the other Domains, as explained below.

1. Performance Architecture – An Agency's Mission Objective (Outcome) will be ensured if the services being delivered are free from any disruptions. The role of Security Architecture here is to be used in the establishment of risk profile for each of the service provided by the Agency and to arrive at an appropriate mitigation strategy. Even if incidents occurred, the protective, detective and corrective mechanisms built into the service infrastructure as well as incident management readiness within the security framework will limit and minimise the impact of such events.
2. Solution/Service Architecture – For each of the service being developed, the Security Architecture is used to define requirements that reflect the threat environments, user profiles and operational metrics that the service infrastructure is exposed to.
3. Information Architecture – Each information asset used or processed within the service will have its own security classification and protection requirements. Data transfers between services will also generate interoperability issues that must be addressed from security point of view.
4. Technical Architecture – The risk mitigation strategy and security requirements derived from the previous three Architectures are then used to implement security mechanisms (technology and processes) as part of the service's technology infrastructure. These mechanisms are put together from components within the Security Architecture Landscape and Technical Control Building Block described in the following sections.

Security Architecture Landscape

The Figure below presents the proposed Security Architecture, along with its Control Groups.

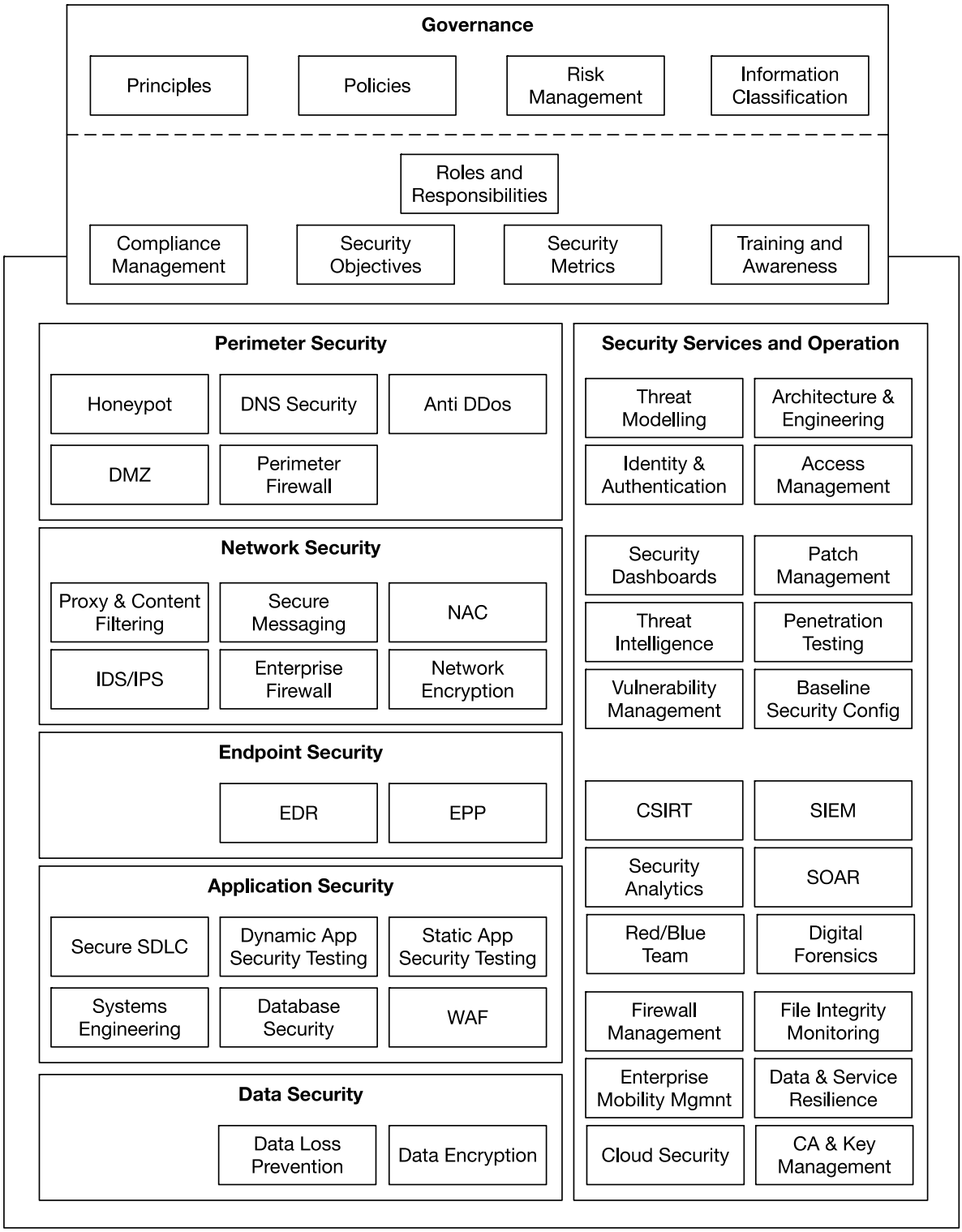

Figure 35 – Proposed Enterprise Security Architecture

Each Group and its component building blocks are defined in the following sections.

Governance

Security governance is the threads that expand and connect all of these building blocks and identifies the practices applied to establish, manage, and enforce information security policy thus allowing the security program to work as a living organism throughout all of the operating units in an MDA.

It also specifies the framework that must be implemented within an MDA for the purpose of interactions with other Agencies, including centralised functions such as those provided by NITA and Ghana Cyber Security Agency.

Reference Framework

- Security Principles – Fundamental decisions and requirements that direct how security should be implemented within an organisation.
- Policies – The statements of required protection of the information objects.
- Risk Management – The total process of identifying, controlling, and mitigating information technology-related risks; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission/business and constraints due to policy, regulations, and laws.
- Information Classification – Provides guidelines to label information by its level of sensitivity and appropriate treatment.

Operational Framework

- Roles & Responsibilities – enterprise-wide roles in managing security tasks and responsibilities for protecting MDA's data and information technology (IT) systems.
- Compliance Management – A management framework to identify and address non-adherence to regulations and established policies across the enterprise. This reduces risk by effectively combining detective and preventive controls to significantly reduce management costs, increase security, and improve asset protection while demonstrating compliance. For this purpose, Internal Audit is defined as an integral part of this management framework.
- Security Objectives – To enable an organization to meet all mission/business objectives by implementing systems with due care and consideration of information technology-related risks to the organization, its partners, and its customers.

- Metrics – framework used to evaluate (measure) whether a security goal/objective has been met by using pre-defined parameters and measuring process. The metrics should be specific, measurable, attainable, repeatable, and time-dependent.
- Training & Awareness – continual program to improve and increase the level of awareness and education in security domain. The initiative should be run and managed as part of an HR development program.

Due to the fundamental importance of the Reference Framework, each of the components will be deliberated in separate sections below.

Security Services and Operations

Implementation of security as an integral part of any IT Services and manage security mechanisms implemented within a particular technology platform. Security should be defined as a baseline for any service being provided to users.

- Threat Modelling – A structured representation of all the information that affects the security of a service or system.
- Architecture and Engineering – Ensure that the Agency's IT systems match their overall business structure, process, mission and goals.
- Identity and Authentication – Ensures those wishing to gain access to information resources are who they represent themselves to be. Typical methods include passwords, smart cards, and biometrics.
- Identity Management – Identity management is the process by which user identities are defined and managed in an enterprise environment. Within a typical security lifecycle this would include account creation, suspension, privilege modification, and account deletion
- Access Management - Determines what permissions and access authorization an information system user holds. Generally, involves the use of procedures and technical controls that limit or detect access to critical information resources.
- Security Dashboards – Analytics to present security performance metrics, security objectives and incidents, allowing continual monitoring and tracking of issues.
- Patch Management – Process of distributing and applying security updates to software to fix or mitigate identified vulnerabilities.
- Threat Intelligence – Framework based on data that is collected, processed, and analysed to understand a threat actor's motives, targets, and attack behaviours.
- Penetration Testing – Carefully planned process to attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

- Vulnerability Management – Management of findings and related corrective actions based on an automated security test that scans a target IP address or service for known and unknown vulnerabilities.
- Baseline Security Configurations – Detail documentation of agreed security configurations to enable the secure by default deployment of particular infrastructure components, operating system, middleware component or application
- CSIRT & Incident Management – The unit responsible for coordinating the response to computer security incidents in an organisation – determines whether or not a security-related incident has occurred and develops methods of control to handle and minimize disruption of service.
- Secure SDLC – SDLC framework that integrates security concerns and analysis into every phase/cycle.
- Event Monitoring & SIEM – is a process of monitoring events within an IT Infrastructure that involves recording information that represents activity and analysing recorded information to identify and respond to questionable activities.
- Security Analytics – A framework that combines software, algorithms, and analytic processes used to detect potential threats to IT systems.
- SOAR – Security Orchestration, Automation and Response – An integrated stack of compatible software programs that enables an organization to collect data about security threats and respond to security events without human assistance. The goal of using a SOAR platform is to improve the efficiency of physical and digital security operations.
- Red/Blue Team – An assessment technique that uses simulated attacks to gauge the strength of the organization's existing security capabilities and identify areas of improvement in a low-risk environment.
- Digital Forensics – A branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically. Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.
- Firewall Management – Centralised process of configuring and monitoring a connected pool of firewalls to maintain a secure network.
- File Integrity Monitoring/Management – Security practice which consists of verifying the integrity of operating systems and application software files to determine if tampering or fraud has occurred by comparing them to a trusted "baseline."

- Enterprise Mobility Management – a set of technology, processes, and policies to secure and manage the use of corporate- and employee-owned mobile devices within an organization.
- Data & Services Resilience – Ability of a system to absorb the impact of the failure of one or more components or a significant disturbance in its environment, and to still continue to provide an acceptable level of service.

  This building block also includes Backup strategy where a duplicate copy of data made for archiving purposes or for protecting against data loss. A backup is considered secure only if it is stored away from the original
- Cloud Security – Procedures and technology that secure cloud computing environments against both external and internal cybersecurity threats. The security mechanisms should be able to cover all categories of cloud computing that may be in use:
  - Public cloud services, operated by a public cloud provider — These include software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).
  - Private cloud services, operated by a public cloud provider — These services provide a computing environment dedicated to one customer, operated by a third party.
  - Private cloud services, operated by internal staff — These services are an evolution of the traditional data centre, where internal staff operates a virtual environment they control.
  - Hybrid cloud services — Private and public cloud computing configurations can be combined, hosting workloads and data based on optimizing factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.
- CA & Key Management

  Certification Authority – An authority that issues and manages security credentials for a PKI framework. Implemented within an organisation to provide centralised CA services for authentication, application signing, messaging and network security.

  PKI - An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys

  Key Management - is the administration of tasks involved with creating, issuing, protecting, storing, backing up, revoking and organising encryption keys used internally within an organisation.

Key Escrow - The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees

Perimeter Security

- Honeypot – Implementation of a controlled and safe environment, a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access.
- DNS Security – Mechanism to security the domain name service and protocol.
- Anti DDoS – Mechanism that uses behavioural analysis, traffic signatures, rate limiting, and other such techniques to identify malicious traffic per source-address and blocks subsequent traffic.
- DMZ – Demilitarized Zone, a network inserted as a "buffer zone" between a company's private, or trusted, network and the outside, untrusted network.
- Perimeter Firewall – Security application that defends the boundary between an organisation's private network from public networks.

Network Security

- Proxy and Content Filtering – Mechanism that allows specific websites or keywords to be blocked, sometimes utilizing a reputation score to determine the safety of a webpage. Proxy filtering uses a server as a gateway to control all incoming and outgoing traffic to safeguard against malicious communications.
- Secure Messaging – secure framework to provide communication services.
- NAC – Network Access Controls
- Intrusion Detection & Prevention – Techniques and mechanism that try to detect or prevent intrusion or unauthorized entry into a computer or network by observation of actions, security logs, or audit data. Intrusion detection is the discovery of break-ins or attempted break-ins either manually or via specific software systems that operate on logs or other information available on the network. Once detection, a prevention mechanism may be put into use to block the originating host or filter further traffic from it.
- Enterprise Firewall – Purpose-built firewall appliances with IPSec VPN capabilities, capable of delivering centralised, extensive firewall and management capabilities for securing tnetwork access across networks.
- Network Encryption – Mechanisms and processes of encrypting or encoding data and messages transmitted or communicated over a computer networks.

Endpoint Security

- Malware Protection – Techniques and mechanism to protect information processing hosts and applications from the effect of malicious software.
- EDR – Endpoint Detection and Response – An integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.
- EPP – Endpoint Protection Platform – Solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Application Security

- Secure SDLC – Collection of best practices focused on adding (integrating) security processes to the standard SDLC.
- Dynamic Application Security Testing – security checking process that uses penetration test techniques on applications while they are running. This is performed without a view into the internal source code or application architecture – it essentially uses the same techniques that an attacker would use to find potential weaknesses.
- Static Application Security Testing – Commonly known as 'white box testing,' implemented to allow software developer team to identify vulnerabilities early in the Software Development Life cycle (SDLC). SAST is performed at the static (pre-production) level ensuring- code guidelines are followed without actually executing the application.
- Systems Engineering – Framework that selects, customises, and assembles components from one or more component systems into complete application systems. These applications are largely constrained to "fit" the architecture and the components.
- Database Security – is the system, processes, and procedures that protect a database from unintended activity. Unintended activity can be categorised as authenticated misuse, malicious attacks or inadvertent mistakes made by authorised individuals or processes.
- WAF – Web Application Firewall

Data Security

- Data Loss Prevention – Framework comprising a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users

- Data Encryption – Mechanism for translating data from plaintext into another form, or code (cyphertext), so that only people with access to a secret key (formally called a decryption key) or password can read it.

Security Principles

The following Security Architecture Principles will guide the planning, design, and selection of security products and services to enable the secure and efficient transaction of business, delivery of services, and communications between Government and citizens, and other MDAs. The principles contained in this document are as a result of technical considerations from operations in Ghana and other organisations around the world.

The principles are:

Principle 1 – Security, confidentiality and privacy

ICT systems should be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.

Rationale:

MDAs process Government and citizen data and use the information to provide services and also make decisions. MDAs such as the Ghana Health Service hold patient information, which must be protected, and therefore Government-wide rules, regulations and policies are required security, confidentiality and privacy of Government data.

Implications:

- Need to identify, publish, and keep the applicable policies current;
- Need to monitor and enforce compliance to policies;
- Must make the requirements for security, confidentiality and privacy clear toeveryone;
- Awareness on information security issues such as privacy and confidentialitymust become a routine part of normal business processes.

Principle 2 – Ability to provide secure e-Government services

The Security Architecture must enable the Government and its MDAs to perform business processes electronically and deliver secure e-Government services to the public.

Rationale:

As the Government embarks on the implementation of e-Government business processes and transactions will continue to increase across the public sector. The Government and its agencies must be able to conduct business processes that provide access to informationand resources electronically, while maintaining confidentiality and integrity. A standard set of security services allows MDAs to focus on business goals rather than on the development and implementation of independent security services.

Implications:

- The implementation of the Security Architecture will:
  - Help protect MDAs' critical assets of resources and information;
  - Provide a framework and foundation for secure interoperability and flexibilityin conducting electronic business across Ghana.

Principle 3 – Applying appropriate security levels

MDAs must be able to apply a level of security to systems and resources commensurate with their value to the MDAs and sufficient to contain risk to an acceptable level.

Rationale:

Security is an e-Government and business process requirement with associated costs. Security costs should be rationalised to the intended benefits of the services that are delivered, and appropriate to the level of security required. The requirements for securitywill vary depending on the MDAs' mandates, individual privacy rights, the application system, connection to other application systems, sensitivity of data, and probability of harm.

Implications:

- Implementation of the appropriate level of security will safeguard against security costs that potentially increase beyond mandated requirements and the value of the assets protected.
- Security must be managed to compliment, not unnecessarily impede the MDA's business operations.

Principle 4 – Maintain security accountability

For auditing and reporting purposes, accurate system date and time are essential to all security functions and accountability and must be maintained.

Rationale:

There is a need for accountability from information security standpoint to enable MDAs capture information from security logs captured from various storage devices for reporting and auditing purposes. The ability to capture security logs is one of the key benefits of using technology for data processing.

Implications:

- The validity of digital signatures and electronic transactions depends on precise, reliable date and time information.
- Audit accountability relies on placing events sequentially according to date and time.

Principle 5 – Must be based acceptable standards

Security Architecture must be based on industry-wide, open standards.

Rationale:

Security Architecture that utilises open standards at all modular levels ensures portability and integration across platforms.

Open standards-based solutions facilitate inter-MDA communications and data exchange and allow adaptability to migrate to emerging security technologies.

Implications:

- Security Architecture services are infrastructure-level services; therefore, to take advantage of security services, application-level security should be designed for open standards.
- Security services already exist for many common applications; however, products from vendors may be implemented in ways that make it difficult to integrate these products into overall security architecture. Existing application, system, or platform security mechanisms should be used whenever they match Security Architecture target standards. Application-specific security mechanisms should only be developed where necessary.

Principle 6 – Protecting Government's security assets

Utilising defence-in-depth and layered security approaches protects the Government's information assets.

Rationale:

Managing Government information security to protect assets must be based on a structured approach

Implications:

- The use of layered security controls across all aspects of network and application better protects resources from various security threats and vulnerabilities, thereby reducing the overall risk of a potential security incident.
- The use of layered security controls and mechanisms better protects the asset if security controls are circumvented.
- Protection of a resource is best accomplished by placing controls as close to the resource as possible. Additional layers of security help to protect the resource in the event that the primary means of protection fails for any reason.

Principle 7 – Interoperability framework

Security is a critical component of individual MDA systems interoperability.

Rationale:

Open, industry-wide standards-based security solutions support interoperability needs between application systems and position MDAs for future interoperability opportunities.

Implications:

- MDAs should use encryption technologies when sharing sensitive data.
- Web-enabled transactions that require user authentication for transfer of sensitive data or funds should use encryption technologies.

Principle 8 – Catering for MDA needs

Security architecture should accommodate varying security needs.

Rationale:

MDA requirements for security vary depending upon the nature of communications, the sensitivity of the information, and the risks to the agency. Security needs will change as business requirements and applications change.

Implications:

- Security services should be granular enough to accommodate the different levels of assurance required, and extensible enough to meet future requirements;
- Resetting security assurance levels should not require modification of the Security Architecture.

- Security Architecture must be flexible to support the introduction and/or integration of new technologies, while maintaining appropriate security protection and meeting statutory requirements.
- Whenever security is required, the location in a communications protocol will have an impact on performance, reliance on an underlying network protocol, and on developers. Choosing the appropriate layer in a communications protocol for security will maximise usability and minimise future changes. The performance impact can be minimised when security services are located in the lower layers of the communications protocol. Services provided at the transport layer have less impact on application programmers than services that run above that layer.

Policies

A security policy is a statement that outlines how each entity accesses each other, what operations various entities can carry out, the level of protection that is required for a system as well as actions that should be taken when these security requirements are not met. The policy is to be formally established and it sets forth rules and processes for workforce members, creating a standard around the acceptable use of the Agency's information technology, including networks and applications to protect data confidentiality, integrity, and availability.

Fundamentally, formally establishing an Agency Information Security Policy will:

- Create a repeatable and consistent process for managing information
- Educate staff members around best practices and corporate security protocols
- Document controls to ensure people adhere to security measures
- Meet regulatory and mission-critical compliance requirements
- Establish guidelines for detecting new threats and mitigating new risks
- Give the public confidence over the Agency's security posture
- Ensure appropriate access to IT and data resources on an "as needed" basis

Each MDA is required to formulate and establish an information security policy that reflects the Agency's tasks, processes, IT infrastructure and objectives.

Risk Management

The GGEA Security Architecture includes Information Risk Management processes for conducting risk assessments and implementing the agreed mitigation strategies. Information security risks are threats that can impact on the availability, confidentially, or integrity of information.

Information Risk Management is about reducing the impact and effect of Government information being compromised by unauthorised disclosure, lack of integrity or availability. The process involves identifying information assets, identifying threats, analysing the risks, developing mitigating strategies and contingencies. An Information Risk Management framework is critical to ensure that an adverse impact of the security of information being compromised on a MDA is reduced to acceptable levels. Information Risk Management must be an integral part of day-to-day operational decision making.

Risk assessment for MDAs will generally include the following elements:

- Identifying threats that could harm and, thus, adversely affect critical MDA operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters;
- Estimating the likelihood that such threats will materialise based on historical information and judgment of knowledgeable individuals;
- Identifying and ranking the sensitivity and criticality of the operations and assets that could be affected should a threat materialise in order to determine which operations and assets are the most important;
- Estimating, for the most critical and sensitive assets and operations, the potential losses or damage to reputation and credibility that could occur if a threat materialises, including recovery costs;
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organisational policies and procedures as well as technical or physical controls;
- Documenting the results and developing an action plan.

The Risk Management process itself include the following:

Understanding organisational context – the first step in the Risk Management process is to understand the MDA's operational environment, to identify and develop an inventory of all the information assets. In understanding the operational environment, the mission and objectives of the MDA will be taken into consideration. The inventory of information assets should cover all assets involved in information processing. Areas to take into consideration are:

- Data;
- Applications;
- Hardware;
- Processes;
- Processing facilities (server room, computer laboratories etc);
- People (staff members directly involved in information processing);

Assets identified in each area should be ranked according to sensitivity and criticality to the nation as a whole and the organisation in particular.

Identifying the threats – a threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. The table below provides a list of potential sources of threats.

Threats	
Physical damage.	**Technical failures.**
Fire.	Equipment failure.
Water damage.	Equipment malfunction.
Pollution.	Saturation of the information system.
Major accident.	Software malfunction.
Destruction of equipment or media.	Breach of information system maintainability.
Dust, corrosion, freezing.	**Unauthorised actions.**
Natural events.	Unauthorised use of equipment.
Climatic phenomenon.	Fraudulent copying of software.
Seismic phenomenon.	Use of counterfeit or copied software.
Volcanic phenomenon.	Corruption of data.
Meteorological phenomenon.	Illegal processing of data.
Flood.	**Compromise of functions.**
Compromise of information.	Error in use.
Interception of compromising interference signals.	Abuse of rights.
Remote spying.	Forging of rights.
Eavesdropping.	Denial of actions.
Theft of media or documents.	Breach of personnel availability.
Theft of equipment.	**Disturbance due to radiation.**
Retrieval of recycled or discarded media.	Electromagnetic radiation.
Disclosure.	Thermal Radiation.
Data from untrustworthy sources.	Electromagnetic pulses.
Tampering with hardware.	**Loss of essential services.**
Tampering with software.	Failure of air-conditioning or water supply system.
Position detection.	Loss of power supply.
	Failure of telecommunication equipment.

Table 10 - Possible Threat Sources

In identifying the possible threats all the information assets must be taken into consideration. All possible incidents or occurrence that could compromise the asset must be noted.

Assessing the Threats – assessing the probability of the threat is the process of trying to ascertain the likelihood of occurrence and ranking them according to the adverse impact it could have on the organisation. Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing.

For example,

- Data is so limited on risk factors around the world and even more so here in Ghana. Factors such as the likelihood of a sophisticated hacker attack and the costs of the resulting damage, loss, or disruption will be very difficult to quantify;
- Costs such as loss of citizen confidence or disclosure of sensitive information, are inherently difficult to quantify;
- Although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented; and
- Information on risk factors is soon out of date due to fast paced changes in technology and factors such as improvements in tools available to would-be intruders.

Possible impact categories are:

- Category I - Death, loss of critical proprietary information, system disruption, or severe environmental damage;
- Category II - Severe injury, loss of proprietary information, severe occupational illness, or major system or environmental damage;
- Category III - Minor injury, minor occupational illness, or minor system or environmental damage;
- Category IV - Less than minor injury, occupational illness, or less than minor system or environmental damage.

Control Recommendations - the final step in Risk Management is deciding how to treat each identified risk. The controls are:

- Risk aversion - the treatment for the risk may be, where practical, not to conduct the activity that creates the risk;

- Transfer of risk- transferring the risk to another party either in full or sharing the risk may be an option in some scenarios. When adopting this solution, risks should only be allocated to the party that can provide the most effective control of the risk;
- Retaining the risk - if the analysis establishes that, taking existing controls into account, the level of risk remains unacceptable, and it is not practical to avoid or transfer the risk, agencies should bear the responsibility of the risk. Controls and detection measures should be then implemented appropriately;
- Reduction of likelihood or consequences -the likelihood of a risk may be reduced through additional controls, which may minimise the frequency of, or opportunity for error, by way of policies and procedures, quality assurance, training etc.
- Monitoring and review - The ongoing review of the information risk environment is critical to overall MDA information management, security and continuity of business. Due to the changing nature of the information environment, new risks will continue to be introduced on an ongoing basis. Changes to the information and business environments may affect the likelihood and consequences of risks and necessitate a change to existing controls.

Information Classification

The following Table describes Ghana's Information Classification based on Confidentiality Aspects

Level	Definition	Example	Policy
0	e-Government transactions that involve no private information content.	A citizen reading or downloading publicly available information from a Government website.	No explicit confidentiality protection is needed at level 0 though care should still be taken to adopt good system practice.
1	e-Government transactions in which the information exchanged is client specific but where the impact of public exposure would be a **minor** resource or nuisance impact on one or more of the involved parties.	Receiving an e-mail indicating that more sensitive information is available for collection from a secure mailbox.	Unpublished private information should be either stored on a system to which only authorised Government users have physical access, or else should be password-protected.
2	e-Government transactions involving private information that could be regarded as sensitive**.**	Electronic filing of income tax and Value Added Tax (VAT) returns. Disclosure of credit card details.	Data stored in a live environment (*eg*. on a database) should be protected by strong access control.
3	e-Government transactions involving private information that could be	Electronic movement of a citizen's medical records. Disclosure of this	Use of cryptography to provide access control is anticipated at this level,

	regarded as very sensitive (substantial).	information to an unauthorised third party might cause substantial distress and damage to the standing or reputation of the citizen.	based on use of a public / private key pair associated with a digital certificate.

Table 11 - GoG Information Classification based on Confidentiality Aspects

.

Technical Control Building Blocks for Security Services

Layered Security itself is a design concept that is often described as "concentric circles of protection" and "compartmentalisation." The idea is to design multiple or concentric layers of security measures so that highly protected assets are behind multiple barriers. Each layer is designed to delay an attack process as much as possible, thus providing protection-in-depth.

When properly planned and consistently implemented, the delay should either discourage a penetration attempt or assist in controlling it by providing immediate notification of an attack-in-progress and sufficient time for an adequate response. To achieve this, controls must be selected so that they complement each other in that if one fails, the other control should offer an alternative means to prevent an attack from progressing or at least provide immediate information (notification) of such failure.

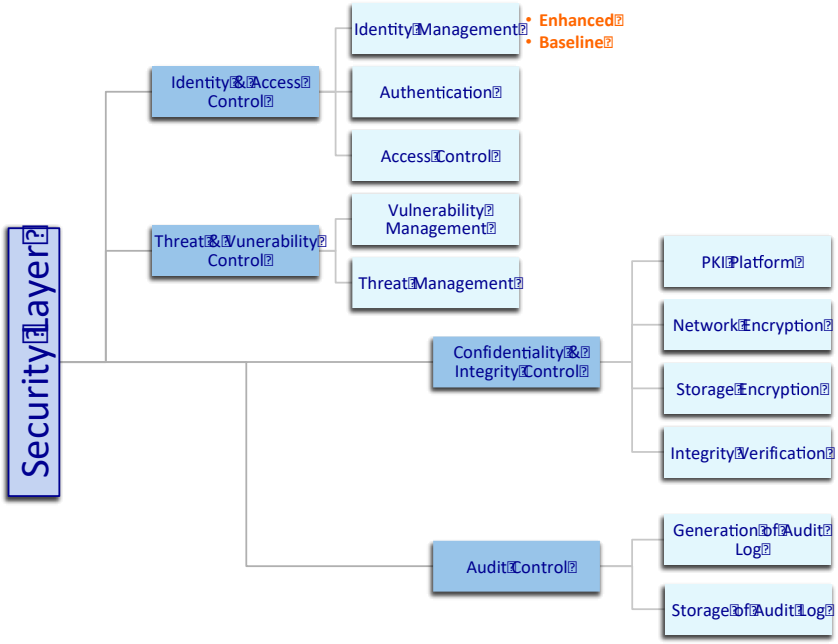

Figure 36 – Control Building Blocks for Security Services

The following sections define the various common technical controls that act as service components or building blocks (see Figure above) and when combined, provide the required layered protection to the objective.

Identity and Access Control

Identity Management
Identity management defines a software platform that manages how humans are identified and authorised across computer networks. It covers issues such as how users are given an identity, the protection of that identity, and the technologies supporting that protection.

Authentication
Authentication defines the security protocol used to confirm the identity of an entity, before subjecting it to authorisation check in an access control system.

Access Control
Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system.

Auditing

Auditing refers to a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event.

Generation of audit log information
Generation of audit log information refers to a mechanism that produces an event log, with sufficient detail, accuracy and validity to be used for the reconstruction and examination of the sequence of events.

Storage of audit log information

Storage of audit log information refers to a mechanism that stores audit log in a secure manner.

Threat and Vulnerability Control

Threat and vulnerability control defines the platform used to prevent occurrence of security incidents by controlling security threat and vulnerabilities.

Vulnerability Management
Vulnerability management refers to software platform used to detect and mitigate discovered vulnerabilities on the affected systems.

Threat Management
Threat management refers to software platform used to detect and prevent security threats such as active attack to the protected systems.

Confidentiality and Integrity Control

Confidentiality and integrity control refers to platform and technologies used to preserve secrecy and authenticity of information.

PKI Platform

PKI (public-key infrastructure) platform refers to software platform that enables the creation, management, distribution, usage, storage, and revocation of digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA).

Network Encryption

Network encryption defines a method to preserve confidentiality and integrity of transmitted information at the network or transport layer.

Storage Encryption

Storage encryption defines a method to preserve confidentiality and integrity of stored information, such as file and/or database.

Integrity Verification

Integrity verification defines a method to attest the integrity of information system and data. File integrity verification is the process of using an algorithm for verifying the integrity or authenticity of a computer file. This is typically performed by comparing cryptographic hashes of the files against a known good reference.

Standards for Security Services

This section describes the control standards that are available for use within MDAs' IT Service Infrastructure. There are 2 (two) standards, Baseline and Enhanced. By default, all service should implement Baseline Security Configuration. The Enhanced configuration may be applied in addition to baseline controls for those services that are related to data with higher security/sensitivity/privacy classification. Controls are defined as being preventive and detective, the former being the more effective of the two.

Network Security Controls

This section defines types of security controls that must be implemented on each corporate network device that forms the logical network zones used by the Service.

1 Identity and Access Control

2 Authentication

- Baseline Security Controls

- **Formal access registration**
  Definition: Formal user registration and de-registration procedure must be in place for granting and revoking user access to a logical zone.

  Access authentication

  Definition: All user and administrative access to a controlled logical zone and network devices must be authenticated and mapped to a specific identity.

- Enhanced Security Controls

  - **Strong authentication factor**
    Definition: The network access devices must be configured to use a strong user authentication factor.

3 Authorisation and privilege management

- Baseline Security Controls

  - **Minimum required privilege assignment**
    Definition: Assignment of rights and privilege level to the network zone and devices must be made based on a need-to-use basis (i.e. the principle of least privilege).

  - **Access policy enforcement**
    Definition: the authorisation access policy must be enforced to all user and administrative access to a controlled logical zone and network devices.

- Enhanced Security Controls

  - **Centralised policy-based network access control**
    Definition: All connection to network access point must be controlled using policy-based access control system that is based on open standard.

  - **Centralised device access control**
    Definition: Administrative access to network devices must be controlled using secure protocol that support centralised configuration.

4 Auditing Control

5 Generation of audit log information

- Baseline Security Controls

- **Authentication audit log:**
  Definition: Authentication process of both user and administrative access to the logical zone and network devices must be logged.

- Enhanced Security Controls
  - **Activity audit log:**
    Definition: User and administrative access post-authentication activities to the logical zone and network devices must be logged to a level that allows complete event and timeline analysis.

6 Storage of Audit Log Information

- Baseline Security Controls
  - **Access control to audit log**:
    Definition: Audit logs must be stored in a securable storage configured with appropriate permission.

- Enhanced Security Controls
  - **Centralised secure logging**:
    Definition: Audit logs must be transmitted and stored in a dedicated machine, in a way that prevents unauthorised, intentional/unintentional alteration and/or destruction.

7 Threat and Vulnerability Control

8 Vulnerability detection

- Baseline Security Controls
  - **Device vulnerability scanning**
    Description: Routine technical vulnerability scanning must be performed against all network devices.

- Enhanced Security Controls
  - **Network vulnerability assessment**
    Description: Network vulnerability assessment must be performed to identify more complex and dynamic vulnerabilities, as well as control-level vulnerabilities

9 Vulnerability mitigation

- Baseline Security Controls

- **Deployment of security updates**
  Definition: Security updates from the device vendor must be applied regularly to mitigate code or binary level vulnerabilities.

- Enhanced Security Controls
  - **Formal change management process for security updates**:
    Definition: Formal change management process must be followed in the deployment of security updates (including impact analysis and fallback procedure).

10 Threat prevention

- Baseline Security Controls
  - **Device security hardening**
    Description: To minimize attack surface and to reduce impact of successful exploitation, configuration of all network devices must be hardened according to an adopted vendor best practice.

- Enhanced Security Controls
  - **Network encryption of device management traffic**
    Description: Remote management access to the network device must be performed over a secure channel.

11 Threat detection

- Baseline Security Controls
  - **System security compliance checking**
    Description: The level of compliance to the adopted security hardening procedure must be verified regularly.

- Enhanced Security Controls
  - **Integrity verification**:
    Description: Integrity of the device firmware and configuration files must be verified on a regular basis using secure hashing algorithm.
  - **Audit log analysis and alerting**:
    Description: Access and activity log should be analysed and alerts should be sent when potential threat is detected.

Application Security Controls

This section defines types of security controls that must be implemented on the main software application used by the Service.

12 Identity and Access Control

13 Authentication

- Baseline Security Controls
    - **Formal access registration**
      Definition: Formal user registration and de-registration procedure must be in place for granting and revoking user access to the application.
    - **Access authentication**
      Definition: All user and administrative access to the application must be authenticated and mapped to a specific identity.
- Enhanced Security Controls
    - **Strong authentication factor**
      Definition: The network access devices must be configured to use a strong user authentication factor.

14 Authorisation and privilege management

- Baseline Security Controls
    - **Minimum required privilege assignment**
      Definition: Assignment of rights and privilege level to the application must be made based on a need-to-use basis (i.e. the principle of least privilege).
    - **Access policy enforcement**
      Definition: the authorisation access policy must be enforced to all user and administrative access to the application modules, binaries, source code, and/or configuration files.
- Enhanced Security Controls
    - **Centralised authentication control**
      Definition: All access to application must be authenticated through a centralised infrastructure based on a secure and open standard.

15 Auditing Control

16 Generation of audit log information

- Baseline Security Controls
    - **Authentication audit log:**
      Definition: Authentication process of both user and administrative access to the application must be logged.

- Enhanced Security Controls
    - **Activity audit log**:
      User and administrative access post-authentication activities in the application must be logged to a level that allows complete event and timeline analysis.

17 Storage of Audit Log Information

- Baseline Security Controls
    - **Access control to audit log**:
      Definition: Audit logs must be stored in a securable storage configured with appropriate permission.

- Enhanced Security Controls
    - **Centralised secure logging**:
      Definition: Audit logs must be transmitted and stored in a dedicated machine, in a way that prevents unauthorised, intentional/unintentional alteration and/or destruction.

18 Threat and Vulnerability Control

19 Vulnerability detection

- Baseline Security Controls
    - **Application vulnerability scanning**
      Description: Routine technical vulnerability scanning must be performed against all of the application accessible interfaces.

- Enhanced Security Controls
    - **Application vulnerability assessment**
      Application vulnerability assessment must be performed to identify more complex and dynamic vulnerabilities, as well as control-level vulnerabilities

20 Vulnerability mitigation

- Baseline Security Controls
    - **Deployment of security updates**
      Definition: Security updates from the application vendor/developer must be applied regularly to mitigate code or binary level vulnerabilities.

- Enhanced Security Controls
    - **Formal change management process for security updates:**
      Definition: Formal change management process must be followed in the deployment of security updates (including impact analysis and fallback procedure).

21 Threat Prevention

- Baseline Security Controls
    - **Application framework security hardening**
      Description: To minimize attack surface and to reduce impact of successful exploitation, configuration of all application supporting framework and/or infrastructure must be hardened according to an adopted vendor best practice.

- Enhanced Security Controls
    - **Network encryption of application data**
      Description: user and administrative network access to the application must be performed over a secure channel.

22 Threat Detection

- Baseline Security Controls
    - **Application framework security compliance checking**
      Description: The level of compliance to the adopted application framework hardening procedure must be verified regularly.

- Enhanced Security Controls
    - **Integrity verification**:
      Integrity of the application binaries, source code, and/or configuration files must be verified on a regular basis using secure hashing algorithm.

    - **Audit log analysis and alerting**:

Description: Access and activity log should be analysed and alerts should be sent when potential threat is detected.

Host Security Controls

This section defines types of security controls that must be implemented on each host (server/workstation) used by the Service.

23 Identity and Access Control

24 Authentication

- Baseline Security Controls
  - **Formal access registration**
    Definition: Formal user registration and de-registration procedure must be in place for granting and revoking user access to the host.
  - **Access authentication**
    Definition: All user and administrative access to the server must be authenticated and mapped to a specific identity.
- Enhanced Security Controls
  - **Strong authentication factor**
    Definition: The host system must be configured to use a strong user authentication factor.

25 Authorisation and privilege management

- Baseline Security Controls
  - **Minimum required privilege assignment**
    Definition: Assignment of rights and privilege level to the host must be made based on a need-to-use basis (i.e. the principle of least privilege).
  - **Access policy enforcement**
    Definition: the authorisation access policy must be enforced to all access to the host operating system binaries and/or configuration files.
- Enhanced Security Controls
  - **Centralised authentication control**
    Definition: All access to the host must be authenticated through a centralised infrastructure based on a secure and open standard.

26 Auditing Control

27 Generation of audit log information

- Baseline Security Controls
  - **Authentication audit log**:
    Definition: Authentication process of all user login attempts to the host must be logged.
- Enhanced Security Controls
  - **Activity audit log**:
    User and administrative access post-authentication activities in the host must be logged to a level that allows complete event and timeline analysis.

28 Storage of audit log information

- Baseline Security Controls
  - **Access control to audit log**:
    Definition: Audit logs must be stored in a securable storage configured with appropriate permission.
- Enhanced Security Controls
  - **Centralised secure logging**:
    Definition: Audit logs must be transmitted and stored in a dedicated machine, in a way that prevents unauthorised, intentional/unintentional alteration and/or destruction.

29 Threat and Vulnerability Control

30 Vulnerability detection

- Baseline Security Controls
  - **Host vulnerability scanning**
    Description: Routine technical vulnerability scanning must be performed against the host.
- Enhanced Security Controls
  - **Host vulnerability assessment**

Host vulnerability assessment must be performed to identify more complex and dynamic vulnerabilities, as well as control-level vulnerabilities

31 Vulnerability Mitigation

- Baseline Security Controls
    - **Deployment of security updates**
      Definition: Security updates from the operating system vendor must be applied regularly to mitigate code or binary level vulnerabilities.
- Enhanced Security Controls
    - **Formal change management process for security updates:**
      Definition: Formal change management process must be followed in the deployment of security updates (including impact analysis and fallback procedure).

32 Threat Prevention

- Baseline Security Controls
    - **Host security hardening**
      Description: To minimize attack surface and to reduce impact of successful exploitation, the host operating system must be hardened according to an adopted vendor best practice.
- Enhanced Security Controls
    - **Network encryption of host management traffic**
      Description: A network access to the host must be performed over a secure channel.

33 Threat Detection

- Baseline Security Controls
    - **Host security compliance checking**
      Description: The level of compliance to the adopted operating system hardening procedure must be verified regularly.
- Enhanced Security Controls
    - **Integrity verification**:

Integrity of the operating system binaries, and/or configuration files must be verified on a regular basis using secure hashing algorithm.

- **Audit log analysis and alerting**:
  Description: Access and activity log should be analysed and alerts should be sent when potential threat is detected.

Data Store Security Controls

This section defines types of security controls that must be implemented on each data store (i.e., database, shared file system) used by the Service.

34 Identity and Access Control

35 Authentication

- Baseline Security Controls
  - **Formal access registration**
    Definition: Formal registration and de-registration procedure must be in place for granting and revoking entity (i.e. user and/or application) access to the data store.
  - **Access authentication**
    Definition: All access to the data store must be authenticated and mapped to a specific identity.
- Enhanced Security Controls
  - **Strong authentication factor**
    Definition: The data store must be configured to use a strong user authentication factor.

36 Authorisation and Privilege Management

- Baseline Security Controls
  - **Minimum required privilege assignment**
    Definition: Assignment of rights and privilege level to the data store must be made based on a need-to-use basis (i.e. the principle of least privilege).
  - **Access policy enforcement**
    Definition: the authorisation access policy must be enforced to all access to the data store system binaries and/or configuration files.

- Enhanced Security Controls
    - **Centralised authentication control**
      Definition: All access to the data store must be authenticated through a centralised infrastructure based on a secure and open standard.

37 Auditing Control

38 Generation of Audit Log Information

- Baseline Security Controls
    - **Authentication audit log**:
      Definition: Authentication process of all login attempts to the data store must be logged.
- Enhanced Security Controls
    - **Activity audit log:**
      User and application post-authentication activities in the data store must be logged to a level that allows complete event and timeline analysis.

39 Storage of audit log information

- Baseline Security Controls
    - **Access control to audit log:**
      Definition: Audit logs must be stored in a securable storage configured with appropriate permission.
- Enhanced Security Controls
    - **Centralised secure logging**:
      Definition: Audit logs must be transmitted and stored in a dedicated machine, in a way that prevents unauthorised, intentional/unintentional alteration and/or destruction.

40 Threat and Vulnerability Control

41 Vulnerability detection

- Baseline Security Controls
    - **Host vulnerability scanning**

Description: Routine technical vulnerability scanning must be performed against the data store.

- Enhanced Security Controls
  - **Host vulnerability assessment**
    Host vulnerability assessment must be performed to identify more complex and dynamic vulnerabilities, as well as control-level vulnerabilities

42 Vulnerability Mitigation

- Baseline Security Controls
  - **Deployment of security updates**
    Definition: Security updates from the data store application vendor must be applied regularly to mitigate code or binary level vulnerabilities.

    Control classification: Logical – Corrective

    Example implementation: deployment of database software security updates
- Enhanced Security Controls
  - **Formal change management process for security updates**:
    Definition: Formal change management process must be followed in the deployment of security updates (including impact analysis and fall-back procedure).

43 Threat prevention

- Baseline Security Controls
  - **Host security hardening**
    Description: To minimize attack surface and to reduce impact of successful exploitation, the data store software must be hardened according to an adopted vendor best practice.
- Enhanced Security Controls
  - **Network encryption of host management traffic**
    Description: A network access to the data store must be performed over a secure channel.

44 Threat Detection

- Baseline Security Controls
    - **Data store security compliance checking**
      Description: The level of compliance to the adopted data store software hardening procedure must be verified regularly.
- Enhanced Security Controls
    - **Integrity verification:**
      Integrity of the data store software binaries, and/or configuration files must be verified on a regular basis using secure hashing algorithm.
    - **Audit log analysis and alerting**:
      Description: Access and activity log should be analysed and alerts should be sent when potential threat is detected.

Protecting Classified Data

Ghana's Government data classification policy defines 4 (four) confidentiality categories (see Section on Information Classification).

When implementing a layered security approach, controls should be implemented such that they provide additional level of protection for data with higher classification.

The following Table describes available control definitions for each data classification based on the technical control building blocks presented in previous sections. However, Implementation strategy should be in line with current Risk Assessment and Risk Acceptance Criteria.

Table 12 – Control Mapping for Protection of Data

	DATA CLASSIFICATION		
	Level 0 – 1	**Level 2**	**Level 3**
	Baseline Security Configuration for Platforms		
Application Layer	IA: Formal access registration IA: Minimum required privilege assignment AC: Limited audit log TVC: Automatic Security Updates	IA: Access Authentication IA: Access policy enforcement AC: Authentication audit log AC: Access control to audit log TVC: Application Vulnerability Scanning TVC: Formal change management for security updates TVC: Application framework security hardening TVC: Application framework security compliance check Application Security Requirements	IA: Strong Authentication Factor IA: Centralised authentication control AC: Activity audit log AC: Centralised secure logging TVC: Application Vulnerability Assessment (Source Code Analysis) TVC: Network encryption of application data TVC: Integrity verification TVC: Audit log analysis and alerting
		Secure SDLC	
Network Layer	IA: Formal access registration IA: Minimum required privilege assignment AC: Limited audit log TVC: Automatic Security Updates	IA: Access Authentication IA: Access policy enforcement AC: Authentication audit log AC: Access control to audit log TVC: Device vulnerability scanning TVC: Formal change management for security updates TVC: Network encryption of device management traffic TVC: System security compliance checking	IA: Strong Authentication Factor IA: Only Access from specific Internal Segments IA: Centralised policy-based network access control AC: Activity audit log AC: Centralised secure logging TVC: Network vulnerability assessment TVC: Integrity verification TVC: Audit log analysis and alerting
Data Layer	Similar implementation of controls as applied in Platform Layer with optional controls base on technology platform (eg. DB encryption)		
Platform Layer	IA: Formal access registration IA: Minimum required privilege assignment AC: Limited audit log TVC: Automatic Security Updates	IA: Access Authentication IA: Access policy enforcement AC: Authentication audit log AC: Access control to audit log TVC: Host vulnerability scanning TVC: Formal change management for security updates TVC: Network encryption of host management traffic TVC: Host security compliance checking TVC: System security compliance checking	IA: Strong Authentication Factor IA: Restricted to Company-approved terminals IA: Centralised authentication control AC: Activity audit log AC: Centralised secure logging TVC: Host vulnerability assessment TVC: Integrity verification TVC: Audit log analysis and alerting

Annex B: GGEA V.2.0 Architecture Governance Framework

This section describes the conceptual and organizational framework for GGEA v.2.0 architecture governance.

The GGEA v.2.0 governance framework which follows is intended to identify effective processes and organizational structures, so that the business responsibilities associated with architecture governance can be elucidated, communicated, and managed effectively.

Architecture Governance Framework Key Concepts

Conceptually, architecture governance constitutes an approach, a series of processes, a cultural orientation, and set of owned responsibilities that ensure the integrity and effectiveness of the organization's architectures. The key concepts are illustrated in the Figure below.

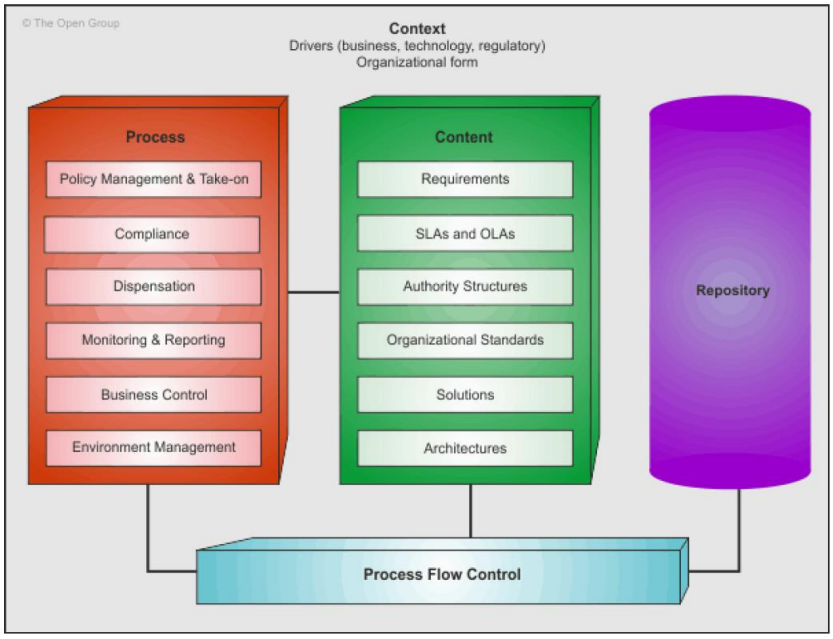

Figure 37 - Architectural Governance Framework - Conceptual Structure

The split of process, content, and context are key to the support of the architecture governance initiative, by allowing the introduction of new governance material (legal, regulatory, standards-based, or legislative) without unduly impacting the processes. A content-agnostic approach ensures that the framework is flexible because processes are independent of the content and implement a proven best practice approach to active governance.

Governance processes are required to identify, manage, audit, and disseminate all information related to architecture management, contracts, and implementation. These governance processes will be used to ensure that all architecture artifacts and contracts, principles, and operational-level agreements are monitored on an ongoing basis with clear auditability of all decisions made.

Continuing governance of architectures yields the following benefits:

- Links IT processes, resources, and information to organizational strategies and objectives;
- Integrates and institutionalizes IT best practices;
- Aligns with industry frameworks such as COBIT for planning and organizing, acquiring and implementing, delivering and supporting, and monitoring IT performance;
- Enables the organization to take full advantage of its information, infrastructure, and hardware and software assets;
- Protects the underlying digital assets of the organization;
- Supports regulatory and best practice requirements such as auditability, security, responsibility, and accountability;
- Promotes visible risk management.

Architecture Governance Key Success Factors

There are three important elements of architecture governance strategy that relate particularly to the acceptance and success of architecture within the GoG. While relevant and applicable in their own right apart from their role in governance, and therefore described separately, they also from an integral part of an effective architecture governance strategy.

1) ***A cross-organizational Architecture Committee*** must be established with the backing of top management to oversee the implementation of the EA governance framework.
2) ***A comprehensive set of architecture principles*** should be established, to guide, inform, and support the way in which GoG sets about fulfilling its mission through the use of IT.
3) ***An Architecture Compliance strategy*** should be adopted - specific measures (more than just a statement of policy) to ensure compliance with the architecture, including Project Impact Assessments, a formal Architecture Compliance review process, and preferably the involvement of representatives of the architecture team in product procurement.

It is important to put in place the following to ensure a successful approach to architecture governance:

- Best practices for the submission, adoption, re-use, reporting, and retirement of architecture policies, procedures, roles, skills, organizational structures, and support services;
- Organizational responsibilities and structures to support the architecture governance processes and reporting requirements;
- Integration of tools and processes to facilitate the take-up of the processes, both procedurally and culturally;
- Criteria for the control of the architecture governance processes, dispensations, compliance assessments, SLAs, and OLAs;
- Internal and external requirements for the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of all architecture governance-related information, services, and processes.

GGEA V.2.0 Governance Roles and Responsibilities

Architecture governance is the practice and orientation by which enterprise architectures are managed and controlled. In order to ensure that this control is effective within the GoG, it is necessary to have the correct organizational structures established to support all governance activities.

The table below presents the roles and responsibilities of the entities that make up the GGEA v.2.0 Governance structure.

GGEA V.2.0 Governance Roles and Responsibilities	
Governance Body	**Roles and Responsibilities**
TBD **[CIO when/if appointed, Director General NITA (DG NITA) in the interim]**	• Approving and issuing the EA Procedure, EA technical standards, and guidance. • Approving and issuing the enterprise architecture and transition strategy. • Approving segment architecture submissions and using architecture to better inform budget and capital planning decisions. • Ensuring GoG compliance with EA policy, Procedures, and Standards.
TBD **[National ICT Steering Committee (NICTSC)]**	• Working with the CIO / DG NITA • Reviews EA, Segment and Solution Architectures prior to approval by the CIO / DG NITA. • Approving and issuing the EA Procedure, EA technical standards, and guidance. • Approving technical feasibility of solution architectures • Approving technical feasibility of transition strategy and sequencing plan. • Ensuring GoG compliance with the EA Policy, EA Procedures, and Standards.
TBD **[Deputy CIO when/if appointed, Deputy Director General Compliance & Standards, NITA in the interim]**	• Deputising for the CIO / DG NITA, as required. • Ensuring EA work is completed in a timely fashion, and reporting on EA progress to the CIO / DG NITA.

TBD [Director EA Directorate / Lead Enterprise Architect (D/LEA) - NITA]	• Leading the development, maintenance, review, and approval of the GoG's enterprise architecture including the baseline architecture, target architecture and transition strategy. • Approving enterprise architecture program management documents (except for enterprise architecture policies, procedures, and standards). • Communicating and implementing approved enterprise architecture documents. • Developing segment architecture priorities and appointing segment and solution working groups, in conjunction with the CIO / DG NITA, NICTMC and the EAWG. • Liaise with MDAs to identify and appoint business subject matter experts to solution and segment architecture working groups. • Providing templates, guidance, and toolsets to support segment and solution architecture submissions. • Certifying and providing documentation of enterprise architecture compliance for segment and solution architectures. • Notifying Segment Architects of upcoming annual enterprise architecture review six weeks prior to commencing. • Facilitating the annual enterprise architecture review.
TBD [Enterprise Architecture Technical Working Group (EATWG)]	• Reviewing and concurring on the enterprise architecture, including, but not limited to the target architecture, transition strategy and sequencing plan. • Agreeing segment architecture priorities. • Reviewing and concurring on enterprise architecture technical standards. • Reviewing and concurring on enterprise architecture compliance standards. • Reviewing and concurring on technical feasibility of technology and security layers of the target enterprise architecture. • Reviewing and concurring on technical feasibility of the transition strategy. • Concurring on enterprise architecture technology standards. • Ensuring compliance with the EA Policy and the EA Procedure.
TBD – Adhoc [Segment and Solution Architecture Working Groups (S/SWG)]	• Leading segment architecture efforts, including developing and maintaining baseline and target segment architectures, and transition strategies using enterprise architecture standards and guidance. • Analyzing across segment architectures during the annual enterprise architecture review and reviewing and recommending solutions to issues identified during the annual enterprise architecture review as appropriate. • Assisting the LEA in the annual enterprise architecture review; evaluating internal and external business drivers that may influence change in the target enterprise architecture. • Reviewing and concurring on enterprise architecture management documents. • Communicating and implementing approved enterprise architecture management documents.
TBD [Deputy Directors / Enterprise Architecture Leads (DDEA/EAL) – NITA]	• Recommending Solution Architects for appointment to Solutions Working Groups • Recommending Segment Architects for appointment to Segment Working Groups • Reviewing solution architectures for project alignment and enterprise compliance • Reviewing and validating segment architectures • Documenting solution architecture enterprise compliance • Requesting enterprise architecture integration of segment architecture • Ensuring Enterprise Architecture Design Documents are created for each piece of architecture work undertaken.

TBD
[Chief Architects (CAs) and/or Principal Architects (PAs) - (Business, Data, Services/Applications and Technology) – NITA]
	• In Segment Architecture:
	  ○ Developing and maintaining their segment architecture using enterprise architecture standards and guidance and ensuring alignment with the enterprise architecture.
	  ○ Reviewing solution architectures project-level reviews and ensuring solution architectures reflect the best practical solution to serving the business needs of the segment while remaining in alignment with the GoG's enterprise architecture.
	  ○ Participating as a member of Segment Architecture Working Groups.
	  ○ Assisting the DEA in the annual enterprise architecture review; evaluating internal and external business drivers that may influence change in the target enterprise architecture.
	  ○ Providing their segment architecture to the DEA for periodic validation and enterprise architecture compliance check.
	  ○ Obtaining waivers from the EA Procedure and the enterprise architecture as appropriate.
	  ○ Completing an Enterprise Architecture Design Document for each segment architecture created.
	• In Solution Architecture:
	  ○ Developing and maintaining their solution architecture using enterprise architecture standards and guidance and ensuring solution architectures reflect the best practical solution to serving the business needs of the segment while remaining in alignment with the segment architecture and the GoG's enterprise architecture.
	  ○ Participating as a member of Solution Architecture Working Groups.
	  ○ Providing their solution architecture for enterprise architecture compliance check during project-level and control gate reviews.
	  ○ Forwarding their solution architecture to the EATC upon completion of project-level and control gate reviews.
	  ○ Obtaining waivers from the EA Procedure where appropriate.
	  ○ Completing an Enterprise Architecture Design Document for each segment architecture created.

TBD **[Enterprise Architecture Directorate Staff (EADS) – NITA]**	• Day-to-day functions of managing and maintaining the enterprise architecture program including developing, updating, and facilitating review of enterprise architecture management documents, standards and guidance. • Lead the development of the EA work products and support environment. • Act as liaison to the business functions. • Integrating segment and solution architectures with the GoG's enterprise architecture following change management procedures. • Providing templates and tools to support architecture submissions for integration with the enterprise architecture. • Facilitating and managing GoG enterprise architecture business processes (including the annual enterprise architecture review), and development of and updates to the GoG target architecture and transition strategy. • Performing analysis across segment architectures and evaluating internal and external business drivers that may influence change in the enterprise target architecture.

Table 13 - GGEA V.2.0 Governance Roles and Responsibilities

GGEA Technical Working Group (EATWG)

Members

#	Name	MDA
1	TBD	TBD
2	TBD	TBD
3	TBD	TBD
4	TBD	TBD
5	TBD	TBD
6	TBD	TBD
7	TBD	TBD
8	TBD	TBD
9	TBD	TBD
10	TBD	TBD
11	TBD	TBD
12	TBD	TBD
13	TBD	TBD
14	TBD	TBD
15	TBD	TBD
16	TBD	TBD
17	TBD	TBD
18	TBD	TBD
19	TBD	TBD
20	TBD	TBD

Table 14 - Enterprise Architecture Technical Working Group Members

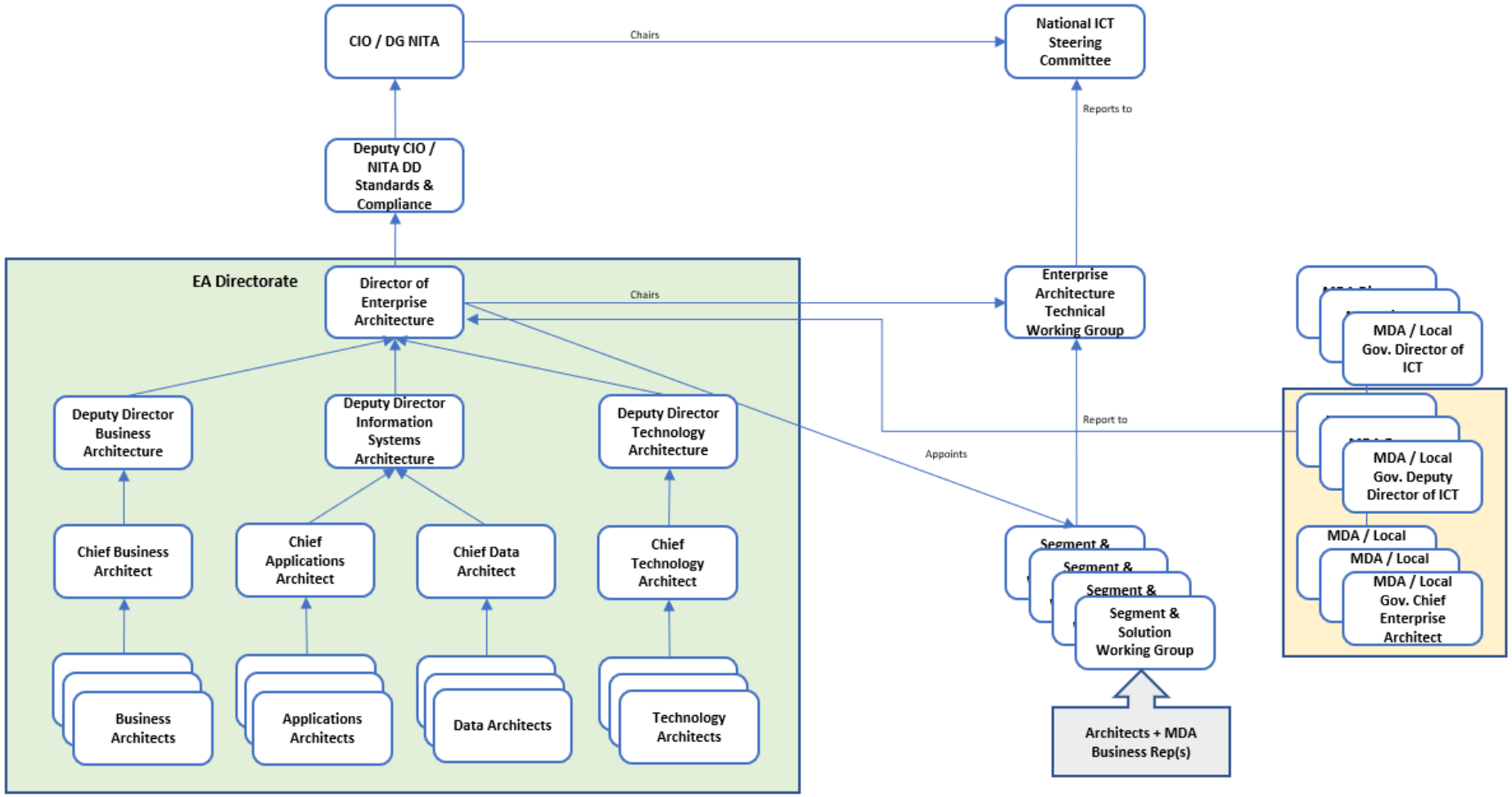

Figure 38 - GGEA v.2.0 Governance Structure

GGEA V.2.0 Governance Framework Content

Architecture Principles

The principles constitute a basic reference point for every IT project and initiative and are drivers for architecture governance. Each new project will be expected to explain how they will conform to the principles and where not, why not. Conformity with the principles will be evaluated before a new application or product is launched and may result in new risks or issues being raised.

GGEA v.2.0 Architecture Governance Processes

GGEA v.2.0 draws on relevant aspects of the TOGAF framework for architecture development and governance. The diagram below illustrates the architecture process, based on the TOGAF ADM, the activities within it and the major inputs and outputs.

The table following the diagram provides a brief explanation of the content of each part of the process.

Detail on the GGEA v.2.0 approach to implementation of the process is provided subsequent to the description of process content.

This is followed by a mapping of the EA Governance processes to the processes of the Prince II Project Management Process, the ISO/IEC 15288 standard for Systems Lifecycle Processes and ITIL – commonly used standards by GoG with which many staff may be familiar.

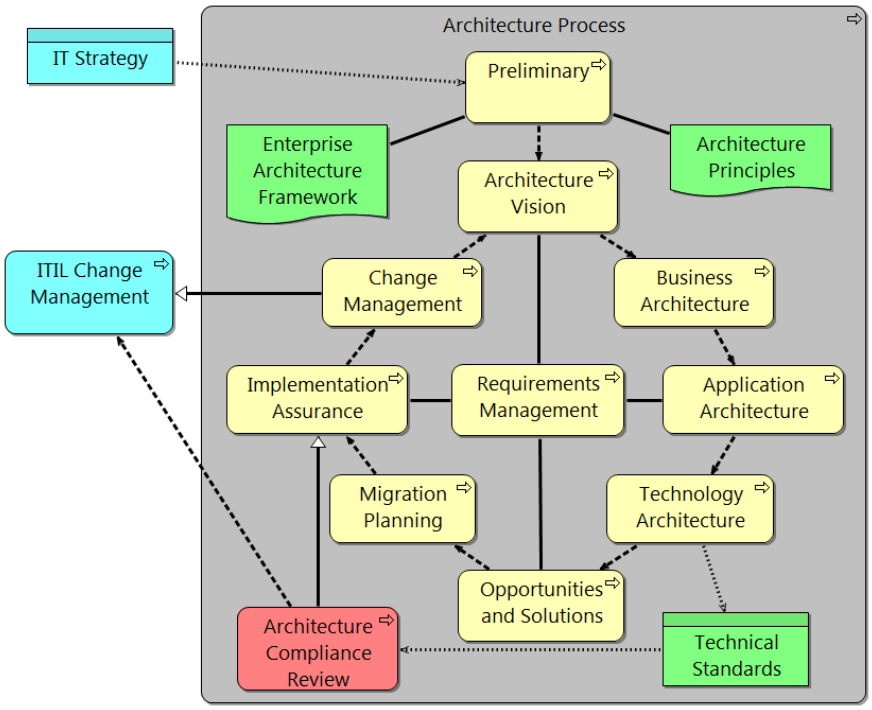

Figure 39 – GGEA v2.0 Architecture Development Process

GGEA v.2.0 Architecture Governance Process Content

Content Type	Description
Application Architecture	Define application architecture including services, major functions, components and interfaces and show how these map to the Business Architecture. Develop logical data models and map to the Business Architecture information models.
Architecture Compliance Review	A critical stage in Implementation Governance consists of a formal Architecture Compliance Review to be held toward the end of the Planning and Implementation Phases of a project. The principal input to the review will be the Architecture Compliance Form or Architecture Description.
Architecture Principles	Enterprise Architecture Principles based on IT Strategy and industry best practice. The principles apply to all IT projects and architecture-related work.
Architecture Process	Generic architecture process based on TOGAF 9 ADM.
Architecture Vision	Set the scope, constraints and expectations for a project or initiative. Create the architecture vision, based on the Architecture Principles, which realises the IT Strategy, aspirations and needs of the GoG. Initiated by a Request for architecture work or via completion of a previous iteration, this activity begins an iteration of the architecture development cycle. For projects, this usually begins in the project Start Up phase and continues into the project Initiation phase with the delivery of an Architecture Compliance Form (ACF) that summarises the proposed solution. Development of the vision usually involves a rapid iteration through high-level business, application and technology architecture activities and results in one or more architecture models to be added to the repository.
Business Architecture	Elaborate business architecture based on the identified business processes, stakeholders, services and capabilities. Develop high-level information models that reflect the underlying enterprise-level informational structures and entities.
Change Management	Changes to the architecture should be managed in the same way as any other system or infrastructure change – using the established change control mechanisms and subject to approval by EA Committee. Architecture Change Management is also a part of the ITIL Change Management process.
Enterprise Architecture Framework	The overarching Enterprise Architecture document that describes the structure and scope of the Enterprise Architecture programme in the GoG.
Implementation Assurance	The Architects will provide ongoing guidance and governance throughout the implementation phase of a project or programme. The basis for governance activities will be the Architectural Principles, Standards and Reference Models that constitute the architecture framework and the compliance of projects as documented in a project Architecture Compliance Form (ACF).
IT Strategy	GoG and/or MDA IT Strategy

Migration Planning	Analyse cost, benefits and risk. Develop detailed implementation and migration plan. The architects will support the project team as necessary.
Opportunities and Solutions	Perform implementation planning and identify delivery vehicles for the building blocks derived from the preceding phases.
Requirements Management	The entire process is based on requirements management. Requirements are identified, stored and input to all activities in the architecture process. This activity is of fundamental importance and needs a rigorous approach, preferably tool-based. Specific and testable requirements must be defined for every system. These constitute design objectives and determine the type of system that will be delivered.
Technical Standards	eGovernment Interoperability Framework (eGIF) containing technical and related standards.
Technology Architecture	Define the infrastructure including computing platforms, storage, networks, operating system, middleware, database systems, other system software and deployable artefacts. Map them to the Application architecture to show how the components, data stores and so-on will be realised. This layer of architecture also encompasses the physical data models and XML schemas that are directly implemented though these will normally be created by the project team

Table 15 – GGEA v.2.0 Governance Process Content

GGEA v.2.0 Governance Processes Detail

This section details architecture development, approval and governance processes of the EA programme for the GoG. The objectives of the Enterprise Architecture Governance Procedure are to define the architecture business processes that support the GGEA v.2.0 and lay out a structured methodology for identifying, collecting, and maintaining architectural information across the GoG. The EA Procedure aims to ensure that EA activities are performed in a consistent, structured, and reusable manner, and direct and inform how investments in Information Technology will be evaluated for compliance with the Enterprise Architecture.

The ways in which the EA Procedure meets its objectives are as follows:

- Develops the EA governance practices as described within the EA Framework to:
    - Define and detail roles and responsibilities for developing and approving GoG's enterprise architecture and supporting artefacts.
    - Ensures GoG participation throughout all enterprise architecture lifecycles.
    - Ensures GoG review and approval at a formal level when agreeing the authoritative enterprise architecture.
- Provides a repository for all artefacts including procedures, standards and tools for maintaining the enterprise architecture available to all interested parties.

- Creates, documents and publishes the review and approval processes which ensures the creation of compliant architectures at all levels (enterprise, segment and solution) including:
    - Review and approval of segment architectures and compliance with the enterprise architecture.
    - Review and approval of solution architectures and compliance with the enterprise architecture.
    - Maintenance, review and approval of the enterprise baseline and target architectures and transition strategies including the introduction of approved solution and segment architectures.
- Enables a process for evaluating the conformance of segment and solution architectures with the enterprise architecture.

Compliance assessments against Service Level Agreements (SLAs), Operational Level Agreements (OLAs), standards, and regulatory requirements will be implemented on an ongoing basis to ensure stability, conformance, and performance monitoring. These assessments will be reviewed and either accepted or rejected depending on the criteria defined within the governance framework.

A Compliance Assessment can be rejected where the subject area (design, operational, service level, or technology) are not compliant. In this case the subject area can:

1. Be adjusted or realigned in order to meet the compliance requirements
2. Request an dispensation/exemption

Where a Compliance Assessment is rejected, an alternate route to meeting interim conformance is provided through dispensations/exemptions. These are granted for a given time period and set of identified service and operational criteria that must be enforced during the lifespan of the dispensation. Dispensations are not granted indefinitely but are used as a mechanism to ensure that service levels and operational levels are met while providing a level of flexibility in their implementation and timing. The time-bound nature of dispensations ensures that they are a major trigger in the compliance cycle.

All architecture artifacts, service agreements, contracts, and supporting information must come under governance through a formal process in order to register, validate, ratify, manage, and publish new or updated content. These processes will ensure the orderly integration with existing governance content such that all relevant parties, documents, contracts, and supporting information are managed and audited.

The governance environment will have a number of administrative processes defined in order to effect a managed service and process environment. These processes will include user management, internal SLAs (defined in order to control its own processes), and management information reporting.

The EA program management structure and EA processes work as the governance foundation for the development, maintenance, and successful implementation of the EA program.

Architecture Development, Review, Approval and Compliance

The following sections describe the roles for developing and the process for reviewing and approving the various architectures. An Enterprise Architecture Design (Compliance) Document will be produced by the architect throughout the architectural work, and be utilised as evidence of compliance during the review cycles of the following processes.

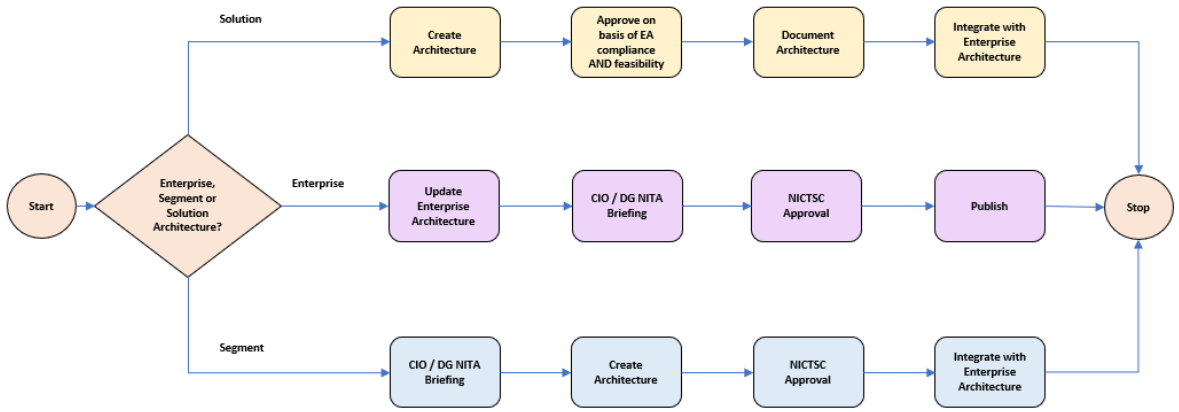

Figure 40 – Governance Process Overview Schematic

Segment Architecture Development, Review and Approval Process

1. On an annual basis, the Director of Enterprise Architecture (DEA), working with the Enterprise Architecture Technical Working Group (EATWG) creates recommendations for segment architecture priorities taking into account any strategic drivers from the CIO / DG NITA and the National ICT Steering Committee (NICTSC). The DEA, following a CIO / DG NITA Briefing between CIO / DG NITA and the EATWG for validation and steering purposes, takes this list of priorities to the NICTSC for approval. The NICTSC approves the segment architecture priorities for the coming year.
2. Deputy Directors of Enterprise Architecture (DDEAs) are accountable for all segment architectures and should utilise internal governance structures to establish best practice.
3. DDEAs assign development responsibility for each segment architecture to a Chief Architect (CA) / Enterprise Architect (EA) as appropriate, and structures governance of each segment architecture based on the size and complexity of each.
4. The CA/EA and Segment Working Group develops the segment architecture, using EA standards, guidance, tools and templates, to address the business requirements for each segment.

5. The CA/EA delivers the segment architecture to the DDEAs for validation. This should be done as the need arises throughout the year to ensure continual alignment with the enterprise architecture. The DEA will notify CA/EAs 6 weeks before the annual EA review in order to allow time for final updates prior to submission.
6. DDEAs review the segment architectures to ensure they address the business requirements correctly or identify areas needing modification.
7. DDEAs submit the validated segment architectures to the DEA to ensure enterprise architecture compliance.
8. The DEA conducts a compliance review to ascertain whether the segment architecture is in alignment with the enterprise architecture using predetermined criteria as defined within the EA standards.
9. If the segment architecture is compliant, the DEA provides approval documentation to DDEAs.
10. If it is not compliant, the EA indicates the areas of non-compliance to the DDEAs. DDEAs will then submit revised segment architecture or apply for a waiver.
11. When compliance is assured (or appropriate waivers secured), the DEA submits the segment to the CIO / DG NITA for approval.
12. DDEAs then forward the segment architectures and request for enterprise architecture update to the CAs/EAs and the EA Directorate.
13. CAs/EAs and EA Directorate integrates it with the GoG's enterprise architecture following suitable change management procedures.
14. The segment architecture can then be used to better inform business planning and forecasting.

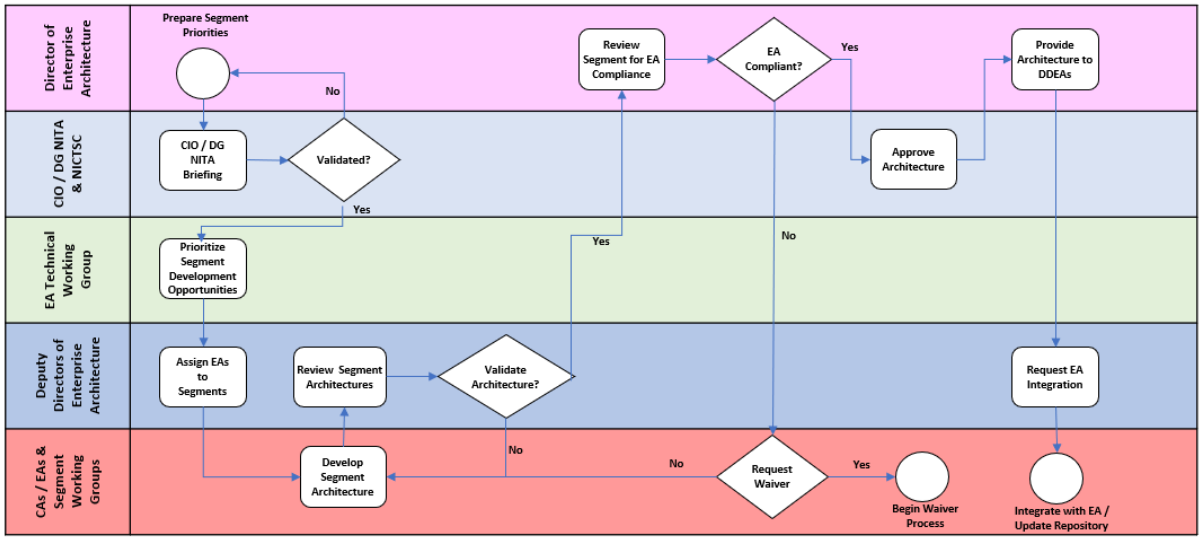

Figure 41 - Segment Architecture Development, Review and Compliance Process

Solution Architecture Development, Review and Approval Process

1. CAs/EAs assigned by DDEAs develop a solution architecture to address a segment's business need utilising EA standards, guidance, tools and templates.
2. The solution architecture is developed and refined over iterative cycles of the ADM.
3. The solution architecture is reviewed after each phase of the ADM. This is a standard development review undertaken by the DDEAs to ensure:
   3.1. Solution architecture accurately addresses the segment's business need; and
   3.2. Checks for continued compliance with the Enterprise Architecture.
4. At the end of the development cycle the solution architecture is sent to the DEA for an enterprise architecture review in conjunction with DDEAs to fully assess enterprise architecture compliance.
5. If the solution architecture is found to be compliant, the architecture is forward to EATWG to assess technical feasibility. If it is not compliant the DEA indicates areas of non-compliance to DDEAs. DDEAs will then submit revised solution architecture or apply for a waiver.
6. DDEAs provide CAs/EAs with EA compliance documentation; this together with the finalised solution architecture is forwarded to the CAs/EAs and the EA Directorate.
7. The CAs/EAs and EA Directorate integrate the solution architecture with the GoG's Enterprise Architecture following suitable change management procedures.

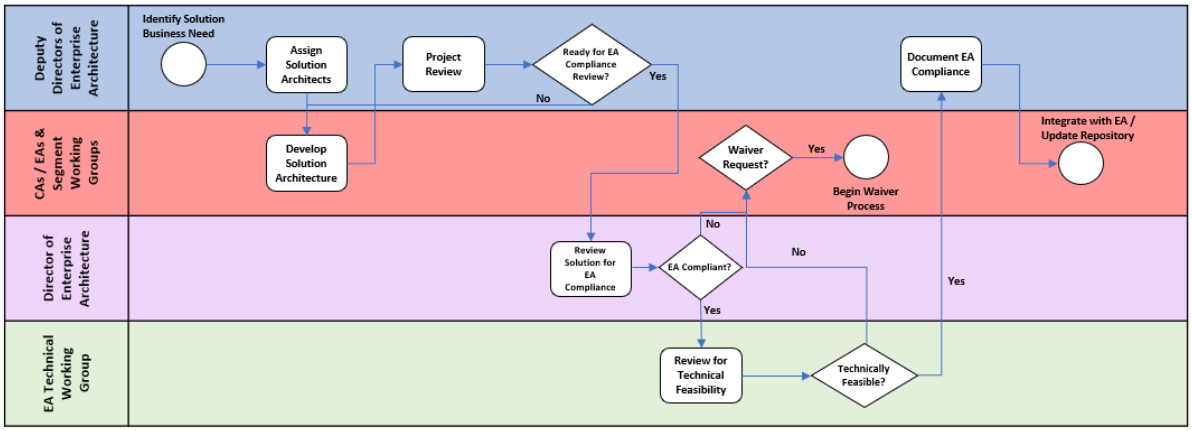

Figure 42 - Solution Architecture Development, Review and Compliance Process

Project Escalation Route

During execution of projects and programmes the standard procedures as set out above should be followed. However, recognising the fact that waiting for the various governing bodies

(EATWG and NICTSC) to convene in order to consider the questions before them may impact negatively on the timescales of executing projects, the following route of escalation is available to the Project Manager (PM).

The Enterprise Architecture Design Document produced by the architect throughout the architectural work will be utilised as evidence of compliance during the escalation reviews in the following process.

In the unlikely event that during the course of project execution the assigned CAs/EAs and PM cannot reach a point of accommodation between project deliverables and the required architecture, the PM may:

1. Escalate the issue to the DEA; if DEA and PM are able to reach accommodation the DEA will inform CAs/EAs and DDEAs accordingly and a revised solution will be worked upon within the project. If accommodation cannot be reached, the DEA will refer the matter to the CIO / DG NITA.
2. CIO / DG NITA will work with the DEA and PM to find accommodation, if reached the DEA will inform CAs/EAs and DDEAs accordingly and a revised solution will be worked upon within the project. If accommodation cannot be reached, the CIO / DG NITA will refer the matter to the NICTSC.
3. The NICTSC, CIO / DG NITA and PM will meet to assess and discuss, and the NICTSC will decide the outcome. The decision of the NICTSC is final.
4. CIO / DG NITA will provide written confirmation of outcome to NICTSC, PM, DEA, CAs/EAs and DDEAs which will be actioned accordingly.

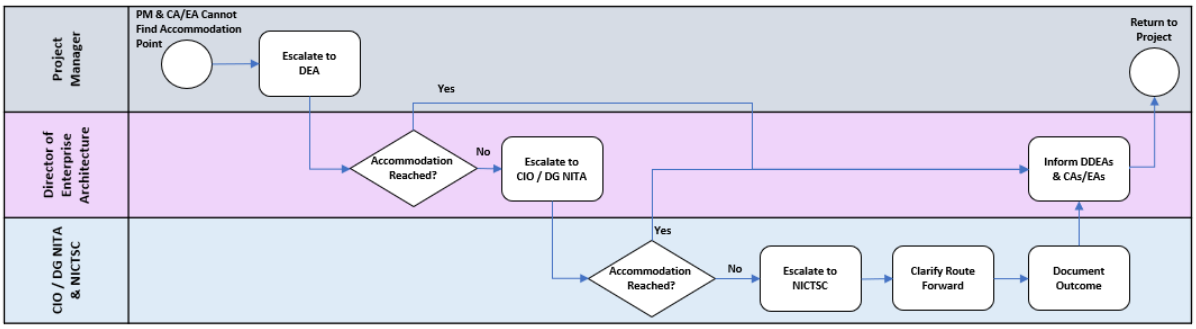

Figure 43 - Project Escalation Route

Integration of Segment and Solution Architectures

Throughout the year upon receipt of approved architectures:

1. The DDEAs and CAs/EAs perform quality assessments of released EA compliant solution and segment architectures.
2. The CAs/EAs and EA Directorate integrate quality assessed, EA compliant segment and solution architectures into the enterprise architecture by authorising change within the architecture repository.

Enterprise Baseline Maintenance

The baseline enterprise architecture is maintained through periodic segment and solution architecture approval. As the enterprise architecture is modified with new segment and solution architectures, the enterprise architecture baseline architecture is populated and updated as a result.

Annual EA Review

1. The DEA and DDEAs draw on strategic planning information to undertake a review of the enterprise architecture; including the baseline and target architectures (segment and solution architectures are included). Based on the findings of this review, the DEA may or may not decide to update the target enterprise architecture to reflect changes in strategic planning or other influencing factors.
2. As the DEA, DDEAs and EA Directorate revisit and refine the target architecture for business, data, application and technology, it is expected that a higher-level version of the Enterprise Architecture Design Document will be produced to reflect the target architecture changes required.

Target Architecture Review and Approval

1. The DDEAs and CAs/EAs redefine and update the enterprise architecture target architecture based on the findings of the annual enterprise architecture review.
2. The DEA reviews the target enterprise architecture and approves or identifies areas for modification to the DDEAs and CAs/EAs.
3. DEA presents enterprise target architecture to the EATWG.
4. EATWG reviews target architecture and concurs or identifies areas for modification to the DEA.
5. DEA presents enterprise target architecture in good time for a briefing with the NICTSC for validation purposes. NICTSC validates design and forwards to CIO / DG NITA for approval via DEA or identifies areas of modification to DEA.
6. DDEAs and CAs/EAs integrate with the EA and update the repository.
7. DEA issues updated enterprise architecture on behalf of the NICTSC and the CIO / DG NITA.
8. Target Architecture is used to inform budget and capital planning.

Transition Strategy Review and Approval

1. The DEA and DDEAs work with the EATWG to define and update the transition strategy based on the findings within the annual enterprise architecture review and any resultant target architecture.
2. DEA reviews the transition strategy and approves or identifies areas for modification to the DDEAs and CAs/EAs.

3. DEA Presents transition strategy to EATWG.
4. EATWG reviews transition strategy for technical feasibility and EATWG concurs on strategy or identifies areas for modification to the DEA.
5. DEA presents transition strategy in good time for a briefing with the NICTSC for validation purposes. NICTSC validates strategy and forwards to CIO / DG NITA for approval via DEA or identifies areas of modification to DEA.
6. DDEAs and CAs/EAs integrate with the EA and update the repository.
7. DEA publishes strategy on behalf of the NICTSC and the CIO / DG NITA.
8. Transition Strategy is used to inform budget and capital planning.

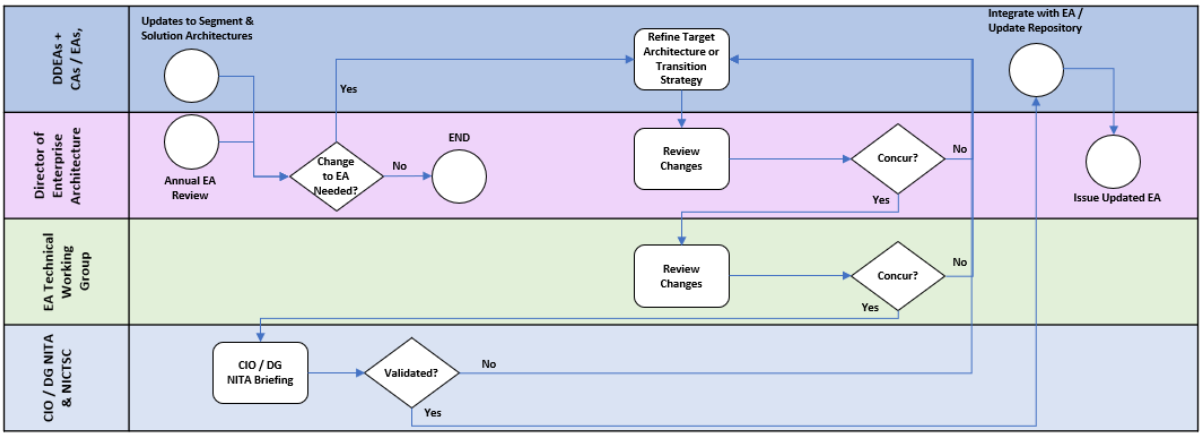

Figure 44 - Enterprise Architecture Review and Approval Process

Architecture Compliance Review

The CAs/EAs will be responsible for architectural governance throughout the project life cycle and will request, via the DDEA, that the DEA organise a formal Architecture Compliance Review (ACR) meeting toward the end of the Implementation phase of a project – preferably when the results of the operational testing are known.

The purpose of the ACR is to verify that the project has not deviated from the agreed architecture and that the system is fit for purpose, conforms to standards and adheres to the Architectural Principles.

Compliance Reviews will be based on a standard agenda and standard terms of reference, which will be published in the Architecture Repository. The attendees should include:

1. **Director of Enterprise Architecture** – organises and chairs the meeting and is responsible for the minutes.
2. **Quality and Security Managers** – or nominated representatives.
3. **Chief/Enterprise Architect(s)** – for the project (can be more than one person) and/or
4. **Project Manager** – if appropriate.

5. **Experts** – from within IT services (e.g., infrastructure or development specialist) as appropriate to the project. Preferably from outside the project team.

The CAs/EAs or PM (as appropriate) will prepare a slide pack and circulate it to the attendees in advance of the meeting, together with any supporting documentation. If the meeting runs out of time to cover the full agenda, a follow-up meeting will be scheduled.

After the meeting, minutes will be circulated to the attendees to give them the opportunity to correct any errors or misunderstandings. The minutes will include the results of the meeting:

1. **Recommendation** – to proceed or stop.
2. **Risks and Issues** – to be recorded in the project Risk Log and Issues Log. These will need to be raised to the NICTSC and may cause delay to the system go-live date or result in an agreed **work-off list** of actions to be completed before the project can be officially closed. Important issues such as major security vulnerabilities may prevent the system from going live at all.

Waivers / Dispensations / Exemptions

When a solution or segment architecture is perceived to be non-compliant with the enterprise architecture the relevant architect may apply for an enterprise architecture compliance waiver.

Requests for waivers from the EA Procedure must be addressed to the DEA acting on behalf of the NICTSC and CIO / DG NITA as set out in an Enterprise Architecture Waiver Policy.

If the waiver is not approved, the architect should create an enterprise architecture compliance plan for approval by the DEA.

Waivers are not permanent. Waiver terms are documented for each waiver specifying:

- Time period after which the architecture in question must be compliant with the enterprise architecture;
- The modifications necessary to the enterprise architecture to accommodate the solution; or
- Some combination of the above.

Whenever a waiver is approved, the DEA and the EATWG will determine if a change to the enterprise architecture is required. If a change is required, the DEA implements measures to accommodate the non-compliant architecture. These changes will subsequently be approved by the NICTSC and CIO / DG NITA during the next annual enterprise architecture review.

The result of a decision surrounding a waiver decision may be appealed to the NICTSC.

Process Comparison

The Architecture Process covers architecture work at the enterprise level as well as at the project or solution level. The following diagram maps it to the Prince II Project Management Process, the ISO/IEC 15288 standard for Systems Lifecycle Processes and ITIL Version 3.

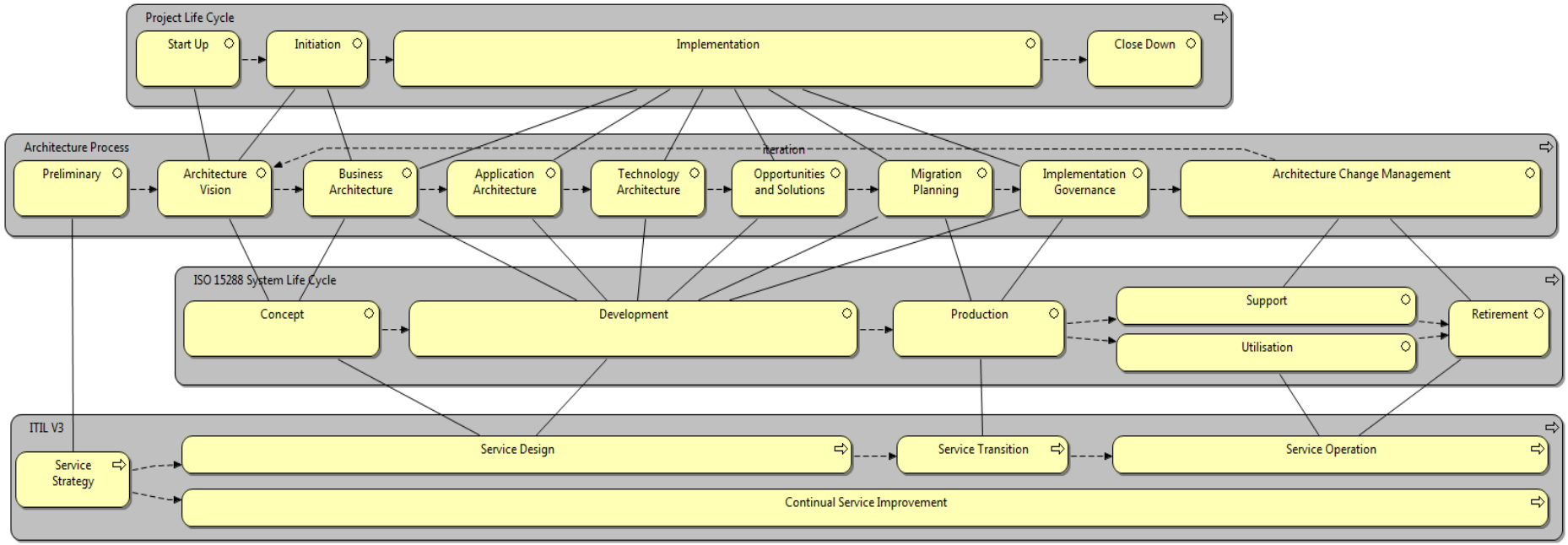

Figure 45 - Process Comparison

While the project life cycle, of course, ends with system go-live, the other processes shown in the diagram must continue for the entire life cycle of the system. ISO/TEC 15288 is a generic system life cycle model used in many industries and is not limited to ICT. It provides explicitly for system Retirement which is covered by Architecture Change Management (TOGAF) and Service Operation (ITIL).

TOGAF and ITIL also cover the initial strategy phase while ISO 15288 is repeated for every system.

Annex C – GoG Enterprise Architects Skill-Set Requirements

The purpose of this section is to define the minimum required Enterprise Architecture skillset for the Government of Ghana. The skills identified in this section are necessary to ensure that EA practitioners are equipped to deliver the services and responsibilities described in ***Chapter 3 GGEA Services and Intended Use***.

This section also provides a comparative analysis of the identified skillset and the industry standard TOGAF EA practitioner skill framework. All skills identified in this section are recommended to be the minimum required skillset that should be incorporated into job descriptions as compulsory core competencies for the position(s) performing the EA function within an MDA.

Skills Development Maturity Roadmap

There are two mainstream views of Enterprise Architecture. The first one is the ICT view that an EA role undertakes the planning responsibilities of the Chief Information Officer (CIO). The second and more contemporary definition is that the EA role focuses on assisting MDAs to identify business opportunities, provide clarity on possible internal and external issues which may affect business execution and aligning the organisation's structural capabilities and performance to reach its desired goals.

Currently, within the GoG, there is a need for strong performance, business and data architecture skills. Technology architecture skills are in greater supply due to a stronger correlation with existing ICT roles.

The Figure below demonstrates the focus of a staff member undertaking the EA role.

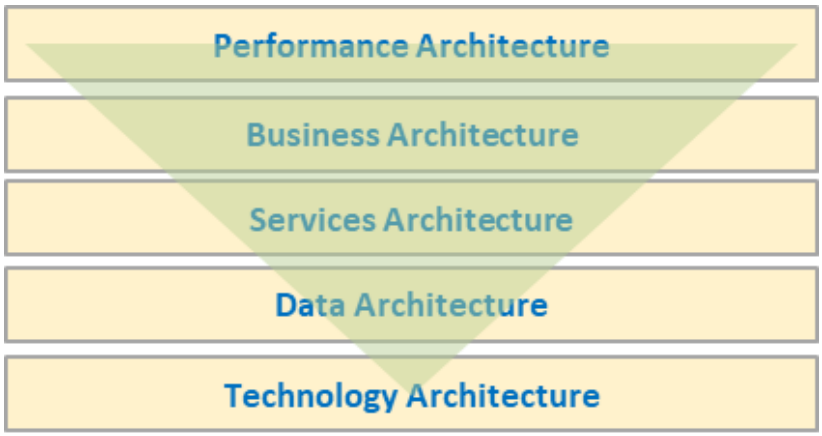

Figure 46 - Enterprise Architects' Domain Focus

The skills required to operate within each domain are similar. The main differentiator is in the depth and proficiency of the skills required to be effective within the requirements of a specific MDA. An MDA's maturity in the adoption of EA as a defined role will go a long way in determining how proficient certain skills need to be.

Identified Skillset

Very few MDAs understand what Enterprise Architecture is and have integrated it into their business and operating models. In most cases, MDAs think of EA as purely ICT related and focused only on managing Technology, as opposed to taking a more holistic, strategic approach to managing their ICT investments. But this is a misconception.

Enterprise Architects are the glue that bridges the gap between business strategy and execution through facilitating enterprise collaboration, not ICT gurus who architect enterprise systems or complex integrated solutions. The Figure below represents the Enterprise Architect's focus towards strategic organisation issues. Note that the EA role is minimal within projects.

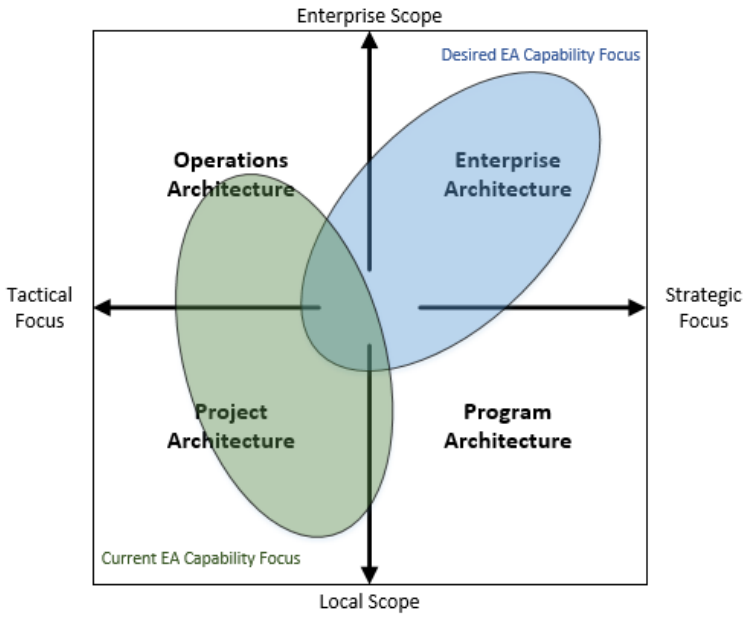

Figure 47 - The EAs' Focus Towards Strategic Issues

With this in mind, the following skills are identified as being required as a minimum skillset for the Enterprise Architecture role within the GoG.

(It is important to note that this section focuses on roles, not positions. A role can be part of a position or spread over multiple positions. A role can be generic, for example "Strategic Planning", or more specific such as a "Business Architect with Health Sector Experience".)

Communication skills

To be effective, staff undertaking the EA role must confidently present messages in a clear, concise and articulate manner to senior executives, business management, ICT management, solution architects, technical architects, Subject Matter Experts (SME), partners and vendors.

EAs need to adapt their vocabulary and style for each situation and target audience to effectively communicate the message they're trying to convey.

They must sell the business value of the structured approach that Enterprise Architecture promotes to an MDA by developing compelling and memorable value propositions and promoting them effectively.

Presentation and public speaking skills

Enterprise Architects are expected to give presentations on a fairly regular basis. As such they need to be comfortable speaking to large audiences, senior executives, business and technical leaders.

They must operate as an effective representative of the MDA in public and internal forums. They must have the ability to translate information for others, focusing on key points and using appropriate, unambiguous language at a level and in a way suitable to the target audiences.

They should be adept at representing complex ideas using suitable tools and techniques to promote a better understanding of the value of the message being conveyed.

Rapport building and networking

EAs must have the ability to build, sustain and influence relationships with key internal and external stakeholders.

A key principle of EA is to break down silos and find common solutions across an organisation. To have any chance of succeeding at this, EAs must network and build rapport with business and technology leaders, SMEs and other influencers.

Ideally, Enterprise Architects should be amongst the most connected individuals in an organisation.

Innovation and creativity

Enterprise Architects are commonly required to find solutions to a wide range of business and technology problems. A good architect has no interest in reinventing the wheel but instead will seek standardised solutions for problems. In cases where no standard solution exists, EAs are expected to determine a simple and sensible solution quickly.

Enterprise Architects may be called upon to find solutions across a wide range of technologies and business domains. Often solutions have budget, time or operational constraints. It takes a considerable amount of creativity and innovation to provide Enterprise Architecture services.

Art of influencing – the Trusted Advisor

Enterprise Architects must be able to build credibility, gain support, inspire others, create relationships and engage people's imaginations to influence their behaviour.

The mandate of EA is ambitious; to bridge the gap between the business and ICT, to break down silos and agree on common solutions. EAs will not be effective in achieving those objectives if they cannot influence others to enact change.

Leadership skills

EAs may be asked to lead business and technology programmes, projects, workshops and initiatives. They must inspire confidence, garner respect from business and technology stakeholders and encourage others to work collaboratively towards a common goal.

Leadership also requires planning, supervision, coaching and delegation skills.

Decision-making

Enterprise Architects are frequently asked to make decisions about technical approaches. The ability to make clear, consistent decisions is key to an EAs success. Decision-making requires skills such as fact finding, big picture thinking, creativity, analytical ability, emotional intelligence and assertiveness.

Negotiating Skills

Enterprise architecture involves building common solutions across organizational, business and technological silos. Implementation and governance of Enterprise Architecture involves constant negotiation. Differences of opinion are the rule, not the exception.

Enterprise Architects must find common ground between stakeholders and determine approaches that have a good chance of gaining stakeholder support necessary to achieve results. Choosing the ideal architectural path needs to be balanced with practical concerns such as budget and time to deployment.

Research Skills

Enterprise Architecture spans business, system, data and technical architecture. To be effective across diverse and constantly changing domains, EAs need to be able to locate, gather, investigate and process information quickly from a variety of sources.

EAs need to explore and proactively research emerging business and technology trends and apply them within the context of their MDA.

Managing Time and Competing Deadlines

Enterprise Architecture involves long term strategic planning. EAs should not be purely reactive; they need to balance daily pressures with the need to focus on achieving long term priorities and goals.

Assertiveness

Avoiding conflict at any cost might be perfectly all right for some professions - an Enterprise Architect is not one of those professions. EAs need to take the initiative, proactively step in and do what is required, question approaches, point out mistakes and ask for help when necessary.

They must challenge important issues constructively and stand by their position when challenged. Effective EAs know it is not possible to please all the people all the time, they are seldom reluctant to speak their mind.

Comparative Analysis against TOGAF Skills Framework

As evidence that the GoG EA Skillset is in line with industry norms, a comparative analysis of the selected skillset against the skillset recommended by TOGAF, the most prominent industry EA framework, appears below.

TOGAF is considered an industry standard for Enterprise Architecture. In the Figure on the following page, the 11 skills identified in this document are mapped against the level of proficiency suggested by TOGAF for generic skills for the EA role.

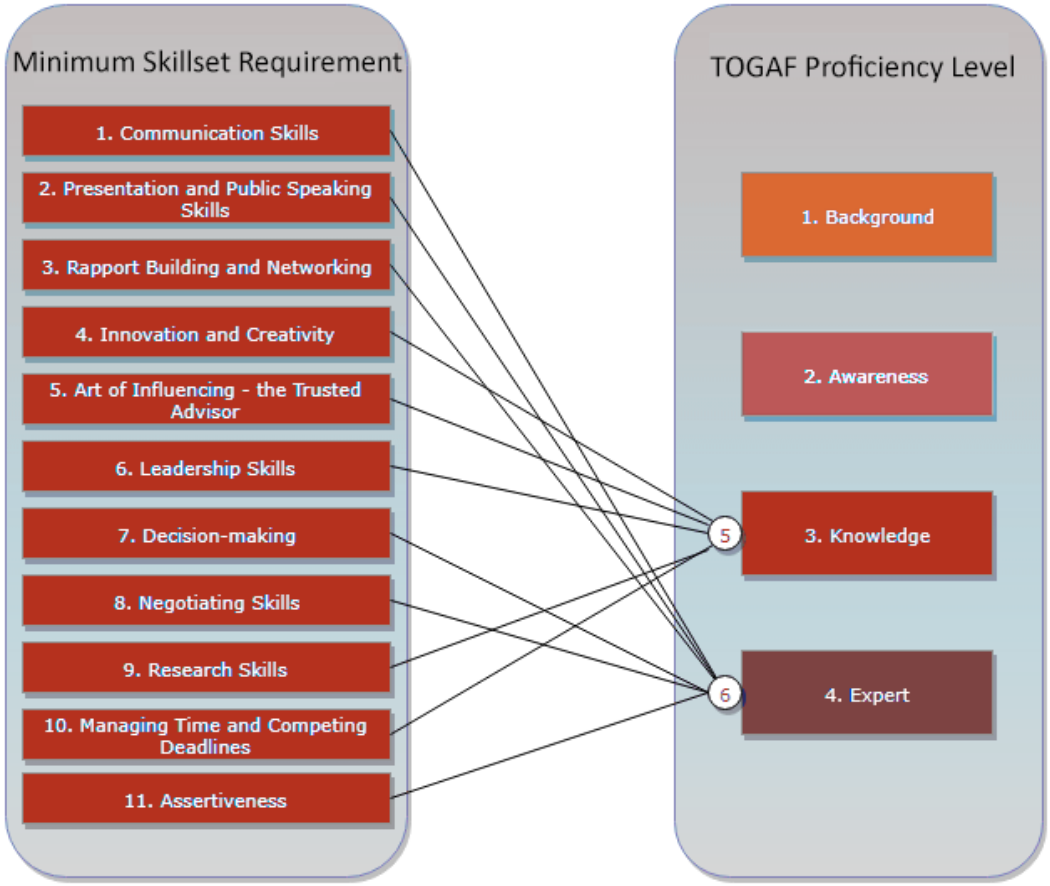

Figure 48 - Mapping of GoG EA Skillset to TOGAF Proficiency Levels