Republic of Ghana

The Ghana E-Government Implementation Strategy

May 2005

Table of Contents

Page

Table of Figures

Page

Section 1. Executive Summary

Good governance and the setting up of government control systems depend on easy access to quality and timely information which also forms the basis of value-added decision-making at all levels of government. Limiting information and knowledge to a few levels of government opens up avenues for its manipulation and unwarranted use for exploitative purposes.

Cognisant of this, the Government of Ghana (GoG) deemed it necessary to find a way of making information and knowledge easily available, not only to all levels of government, but also to its citizens and businesses to ensure that they are properly empowered to become part of the governmental decision-making process – a process that affects them both directly and indirectly.

This pervasiveness in knowledge availability can be achieved by digitizing the entire set of knowledge within a network which links every individual and gives democratic rights to everyone to access and make use of this knowledge. This digital network will form the platform for governing the country electronically in a manner globally known as E-Government (or electronic Government). E-government means the use by the government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to:

- Enhance the access to and delivery of government information and services to the public, other agencies, and other government entities; or
- Bring about improvements in government operations that may include effectiveness, efficiency, service quality, or transformation

E-government will improve productivity in government administration and service delivery by facilitating exchange of information in a standardized format, thereby enabling better interaction and coordination of work among Ministries, Departments, and Agencies (MDAs), citizens, and private businesses. E-governance is intended to change the way government interacts with citizens (Government to Citizens - G2C), with businesses (Government to Business - G2B), and with itself and other governments (Government to Government - G2G).

To establish a framework for GoG to modernize its Information and Communications Technology (ICT), and also as a precursor to e-government, GoG has come out with an ICT policy document referred to as ICT for Accelerated Development (ICT4AD), which identifies fourteen (14) priority areas that should be addressed to enable GoG develop the ICT sector and industry as well as use ICT to achieve its developmental goals, such as the Ghana Poverty Reduction Strategy (GPRS). One of these priority areas is to promote e-government and/or e-governance. This document seeks to formulate a strategy that will provide a direction for the implementation of e-government.

To succeed in the implementation of e-government, it is imperative to proceed in a structured manner by meticulously identifying practical opportunities, establishing pertinent frameworks, and outlining specific programmes and instructive plans that will comprehensively guide the implementation. Accordingly, the strategy identifies six (6) strategic goals. The first of these is to establish an institutional framework – an E-Government Management Structure (E-GMS). The E-GMS will review the e-government strategy, plans and actions, and oversee their implementation. Additionally, the government has to establish ICT Services Divisions/Directorates ~~to~~ in each MDA. A *National E-Government Implementation Committee* made up of the Head of the E-GMS and the Heads of the ITSDs among others is to be set up with an oversight responsible for the implementation of the E-Government programme nationally.

The second strategic goal focuses on the establishment of a component-based Ghana Government Enterprise Architecture (GGEA), a framework comprising five (5) interrelated reference models designed to facilitate cross-MDA analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across MDAs. The reference models are the:

- **Performance Reference Model (PRM):** establishes monitoring and evaluation mechanisms for measuring e-government implementation and MDA operation efficiency and effectiveness.
- **Business Reference Model (BRM):** identifies opportunities to simplify processes and unify work across MDAs and within lines of business in government.
- **Service Component Reference Model (SRM):** identifies opportunities to deploy common and specific applications, and establishes a foundation for the re-use of applications, application capabilities, and components across MDAs and within lines of business in government.
- **Technical Reference Model (TRM):** establishes policies, standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components. The secure delivery of these components will, at a minimum, be based on the key security concepts of confidentiality, availability, and integrity, and a trust collaboration infrastructure.
- **Data Reference Model (DRM):** identifies data and information that will support MDA and government operations and establish a repository, which holds data about government data.

The third strategic goal seeks to implement a secure, robust, and interoperable E-Government Infrastructure for communications, networks, servers, information and knowledge, Internet and web services, applications, and security.

The fourth strategic goal exhorts GoG to ensure that the Legal and Regulatory Framework that supports E-Government adoption and implementation. Access to privileged information has to be regulated. Web content needs to be regulated to

forestall display of pornographic and other offensive material. Citizens rights needs to be protected, and privacy of personal information assured.

The fifth strategic goal seeks to leverage the use of ICT, within an effective E-Government Environment, to meet vital socio-economic development goals such as: improving governance, alleviating poverty, providing basic health care, enhancing education, improving agriculture, providing an enabling climate for small and medium sized enterprises, and enhancing the law and judicial processes

The sixth and final strategic goal requires the government to encourage the active and direct participation of the private sector in the implementation of E-Government. Participation could be in the form of assistance in the processing of bidding documents for equipment and services, supplying hardware and software on easy terms, maintenance and technical support of equipment, and conversion of paper-based information to digital information stored in databases.

Having established the strategic E-Government goals, the change processes (phases) that the E-Government Implementation has to undergo have been identified as MDAs establishing web presences initially and then constructing fundamental E-Government building blocks (such as infrastructure, middleware, a metadata repository, and reference models).

Next, the E-GMS ought to see to the extension of the capability of MDA websites to allow people and businesses to interact with government by completing and submitting forms on-line. After this, MDAs should add self-service capabilities to their websites so that people can complete entire transactions (execute events, decisions, and payments) or processes on-line.

Finally, E-Government implementation should seek to transform the way government operates by integrating governmental processes across traditional boundaries, customizing information and services to the particular needs of individuals and businesses, and allowing people and businesses to access information and services through a single point of contact on the web.

Some of the key implementation challenges identified are: the need for citizen to trust government (and vice versa) regarding online interaction and transactions, inadequate bandwidth and consequent exorbitant tariffs charged by communication monopolies, Ghana's low tele-density of 4% (March 2004), poor quality of data and information management practices in MDAs, limited interoperability of MDA systems, the digital divide, finding adequate funding for E-Government programmes, building capability in MDAs and the citizenry, public education and participation, measuring the uptake and effectiveness of E-Government, protecting E-Government sites from attack, and ensuring that laws are updated to recognize electronic documents and transactions.

In spite of all the benefits that E-Government can bestow on MDA operations and the gains that the citizenry and businesses can derive from it, it is important that E-Government is not seen as a panacea to all the country's governance and administration problems. E-Government should not be expected to be a quick and

simple process that will happen just because MDAs buy more computers and put up a website. Neither will it solve all problems of corruption and inefficiency. Furthermore, it will not overcome all civil engagement barriers.

Successful E-Government implementation depends on the active participation of citizens and businesses, teamwork, strong and visionary leadership, political and governmental support at the highest level, adequate funding, strong methodological support, strong and effective operational management, continuous coordination and feedback at all stages of implementation, highly qualified ICT professional, sustained and extensive training and education of MDA personnel, change management, risk identification and mitigation, and an appropriate legal and regulatory framework.

Section 2. Introduction

The Government of Ghana recognises that, in the new emerging economic order, information and knowledge are now the fundamental bases for wealth creation and national prosperity. Today, more than ever, information is considered a primary resource essential to the operation of a country's economy. Information and knowledge-based economies are generating opportunities in many developed and developing countries for the creation of quality jobs, rapid economic development, and the means to facilitate global competitiveness. The emerging information revolution will be a key factor for achieving progress in economic and social development in the country.

GoG believes that ICT offers the country a critical tool to advance the key stages of industrialisation and transform an agriculture-dominated economy into a service-sector economy driven by high value-added information and knowledge-based technology that can compete on the global market. Government also recognises the need to improve the capacity and effectiveness of public institutions through the ICT use.

Governments all over the world have recognized E-Government and governance as important initiatives for improving government service delivery to the public and bringing government closer to the people. Consequently, GoG is developing a strategy for E-Government to enable it stay abreast with these developments.

The civil and public services play a key role in the socio-economic development process of Ghana. And the crucial role that ICT can play in improving the efficiency of delivery of government services, in reducing (in the long run) the operational cost of these institutions, and in bringing government closer to the people has been acknowledged.

The deployment and exploitation of ICTs to support the operations and activities of the civil and public services has been recognized as key to the institutional renewal, re-engineering and the modernization of the civil and public service.

People are becoming more aware of their rights and the opportunities that lie ahead of them and are developing capabilities to make informed choices in all areas which influence them, including the sphere of Governance.

In this wired-up era, the inhabitants of the knowledge societies will increasingly have freedom, flexibility and opportunities to decide how they would like to be governed and by whom. The underlying truth will become self-evident that – *it is not the leaders who govern people but it is the people who let the leaders govern them.*

The multiple roles of government, at all levels, must be recognized and understood if it is to be effective in this partnership involving access to ICT.

In effect, government:

- uses information and information/communication technology provided by the private sector for public administration
- produces public information to which citizens must have access, and
- has the authority to establish marketplace rules and put in place regulatory structures that ensure that everyone participates and benefits from growth of the knowledge economy.

There is an inextricable relationship between the government role as a user of ICT and its capacity to formulate public policy for the knowledge economy. Governments that learn how to use these technologies to operate more efficiently and improve public services are more likely to effectively stimulate and contribute to the knowledge economy public policy debate. Online delivery of services benefits both government and its constituents. It also lowers costs and makes services more accessible.

Purpose

The purpose of this document is to provide an approach to initiating, implementing, and sustaining an efficient, economic, and effective government-wide electronic means of sharing information and knowledge, in order to facilitate GoG's delivery of services to Ghanaians.

Scope

The document gives guidelines to facilitate and direct the development and implementation of a comprehensive E-Government and governance strategy for Ghana. This will enhance service delivery, productivity, and reduce operational cost by improving on its organizational systems, structures, procedures and processes. The modernization will also allow citizens and businesses to interact with government and participate in the government decision-making. It is also expected that the document will help facilitate the establishment of an efficient intra-and inter-departmental, inter-sectoral, national and sub-national system of communication, for the necessary feed-back in policy formulation and programme implementation, monitoring and review.

The Terms of Reference (ToR) that spawned the creation of this document will be found in Appendix A.

Acknowledgements

In developing the document the E-Strategies of other countries, such as New Zealand, Australia, United States of America, the United Kingdom, Canada, Bulgaria, Germany, Brunei, the Philippines, and the Denmark have been extensively consulted and material extracted from them.

Background

The need for an E-Government Strategy for Ghana is based on the premise that in the new information age, the use of *information*, *knowledge* and *technology* can improve the socio-economic development fortunes of a nation. This will allow such nations to move faster on the socio-economic development scale compared to others. In the new emerging economic order it is now acknowledged that the fundamental basis for wealth creation and national prosperity has now shifted to information and knowledge and Ghana cannot afford to be without either of these.

Ghana has since the mid 1990s taken a number of policy steps to liberalize the telecommunications and communications sector aimed at promoting the development of the nation's ICT infrastructure and improve universal access and service. As part of this process and within the context of developing an 'ICT for Development' policy for Ghana, efforts were made to create a harmonized strategy in which ICTs could be used to transform the operations of the civil and public service in addition to creating avenues for the citizenry to interact with Government. All these efforts have culminated in the ICT for Accelerated Development (ICT4D) Policy document approved by the Cabinet and Parliament in 2004.

Efforts made to-date to facilitate the deployment of ICTs for government administration and service delivery have encountered many implementation challenges including the lack of expertise among the Ministries, Departments and Agencies (MDAs) staff to implement such projects.

Within Government, there is no government-wide infrastructure to facilitate the exchange of information among the various MDAs. Some small networks exist, such as those of Public Financial Management Reform Project (PUFMARP) and other agencies, which link only a few MDA's. The absence of such information infrastructure hampers the roll out of information systems that can be used to modernize the operations of government.

Due to the absence of a government-wide information infrastructure, "stand-alone" applications are the prevailing mode. Only a few MDAs operate on Local Area Networks (LANs). There is minimal use of groupware or workgroup applications, executive information systems, and decision-support systems, which generally add value to ICT applications because they facilitate communication and information sharing, and could potentially improve the efficiency and efficacy of government agencies. There are no mission-critical systems fully operating on enterprise -wide networks or linked with other information systems of other agencies. Sharing of databases or communication network has not been vigorously explored or adopted within government. In addition, ICT planning and procurement are done in isolation, thus preventing the setting up of needed integrated application systems that cut across different MDAs.

The adoption of an E-Government Strategy, which includes measures for inter-connectivity of all MDAs, will facilitate information exchange and sharing among them.

ICT expertise and know-how are a vital component of the support infrastructure for any organization. Developing and maintaining computerized information and communication systems require a large pool of competent ICT professionals for systems beyond office productivity and clerical applications. Unfortunately, Ghana does not have many of such professionals. There is therefore a need for a coordinated approach to providing quality technical support to all the MDAs. An E-Government strategy should address this critical need.

At present, most government agencies are essentially left to themselves to establish or adopt available ICT industry standards. While most internationally recognized standards for hardware, software, and data communication protocols and equipment can be adopted readily or with certain modifications, the establishment of data and application standards is equally important. Having common data and application standards in government is essential for compatibility, for sharing databases, and minimizing redundancy and inaccuracies in common and/or integrated applications.

The challenge, therefore, is to ensure interoperability and compatibility among the different information and communication systems of government. The immediate task is to formulate, disseminate and enforce a common set of ICT standards for all government organizations.

There is therefore the need for an E-Government Strategy that will articulate the vision of ICT development in the public sector, and its role in achieving socio-economic development goals and in pursuing more efficient, effective and responsive governance.

This strategy must also define and establish ICT development priorities, particularly those relating to financing and investment.

There is a need to formulate technology, security, interoperability, functionality, and other relevant standards and benchmarks, as well as guidelines, for the implementation of the E-Government Strategy.

As part of the strategy to strengthen the local ICT industries, an E-Government Strategy is needed that will define an outsourcing policy which will ensure that Government gets the best service for the least value. Towards this end, the strategy should help the government to develop policies that stimulate competition, upgrade the capacities of local industry, and explore the potential of opening the government ICT market.

In effect, the E-Government strategy to be developed will address many of the challenges facing MDAs in their effort to enhance their operations.

Document Organisation

This strategy document has been organised as follows:

Section 3. What is E-Government?

This section deals with defining E-Government and goes on to explain the basic differences between E-Government, E-Business, and E-Commerce.

Defining E-Government

E-Government (electronic Government) means the use by the government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to:

(a) enhance the access to and delivery of government information and services to the public, other agencies, and other Government entities; or

(b) bring about improvements in government operations that may include effectiveness, efficiency, service quality, or transformation

E-Government uses digital technologies to transform government operations in order to improve their effectiveness and efficiency, and service delivery. It builds links between government entities, their customers and suppliers, connecting jurisdictions, departments, customers, and locations. It involves taking processes currently functioning and new processes identified within government and optimizing them using ICT.

The E-Governance Concept

Good governance rests on the pillars of knowledge and the use of this knowledge by the decision-makers. Digitization of this entire set of knowledge within a network, which links every individual including the decision-makers and gives democratic freedom to everyone to access and make use of this knowledge paves the way for E-Governance. Introduction of E-Governance is a way to ensure that common citizens have equal rights to be a part of the decision-making processes, which affect them directly or indirectly, and influence them in a manner that best improves their conditions and the quality of lives.

While E-Government entails delivery of government services and information to the public using electronic means, E-Governance allows direct participation of constituents in government activities. E-Governance is not just about government web site and e-mail; about service delivery over the Internet; or about digital access to government information or electronic payments. *E-Governance is intended to change the way that:*

- *government interacts with citizens (G2C)*

- *government interacts with businesses (G2B), and*
- *how governments interacts with itself and other governments (G2G).*

E-Governance is therefore the use of ICTs to support good governance. These new connections strengthen existing relationships and build new partnerships within civil society. E-Governance therefore embraces:

- *E-Administration*: improving government processes by:
  - cutting costs
  - managing performance
  - making strategic connections within government, and
  - creating empowerment.
- *E-Citizens and E-Services*: connecting citizens to government by:
  - talking to citizens and supporting accountability
  - listening to citizens and supporting democracy, and
  - improving public services.
- *E-Society*: building interactions beyond the boundaries of government by:
  - working better with business
  - developing communities
  - building government partnerships, and
  - building a civil society.

E-Governance aims at bringing forth new concepts of citizenship, both in terms of needs and responsibilities; allowing citizens to:

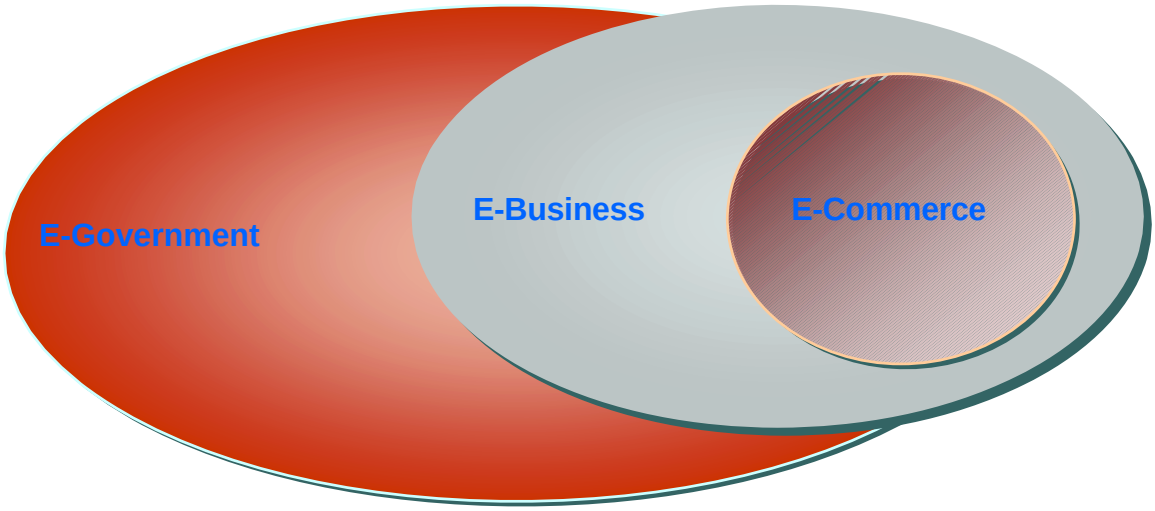
- communicate with government
- participate in the government's policy-making
- communicate with each other; and
- participate in the government decision-making process

reflecting their true needs and welfare by utilizing E-Government as a tool.

The basic differences between E-Government, E-Business, and E-Commerce

Figure 1 on the next page depicts the interrelationships between E-Government, E-Business, and E-Commerce. E-Business embodies E-Commerce and overlaps (or interacts with) E-Government.

Figure 1: E-Government, E-Business, and E-Commerce



E-Government, E-Business and E-Commerce are amplified further in the next few paragraphs.

E-Government

E-Government is using electronic information to improve performance, create value and enable new relationships between government and its customers.

E-Government creates new sources of stakeholder-value by:

- achieving superior service
- portraying a better image of government
- reducing costs
- providing single windows of service
- defining new services
- managing risk and compliance, and
- leveraging human capital.

E-Business

E-Business is concerned with improving business performance through connectivity by:

- deploying new technologies in the value chain to achieve transparency and visibility
- connecting value chains between and across businesses, and between business and consumers, in order to:

- improve services
- reduce costs, and
- open new channels, thereby transforming competitive landscapes in businesses.

E-Commerce

E-Commerce embodies the marketing, selling, and buying of products and services on the Internet.

Section 4. Why an E-Government Strategy?

The government has now published the Ghana ICT4AD policy document. This document takes into account the aspirations and the provisions of key socio-economic development framework documents including:

- the Vision 2020 –The First Steps
- the Ghana Poverty Reduction Strategy (GPRS 2002 -2004), and
- the Co-coordinated Programme for Economic and Social Development of Ghana (2003-2012).

The ICT4AD policy document identifies fourteen priority areas (see Appendix B) that should be addressed to enable GoG develop the ICT sector and industry as well as use ICT to achieve its developmental goals. The portions of this document that refers to the ICT policy have been referenced in Appendix C of this document.

The development of an E-Government Strategy will be necessary in accomplishing the objectives of priority area 3 - *Facilitating Government Administration and Service Delivery – Promoting Electronic Government and Governance.* The success of any E-Government activity within the government will depend on proceeding, in a structured manner, with specific programmes and plans derived out of the strategy document.

An overall framework is therefore required which clearly defines the E-Government initiative and into which the individual E-Government activities of the various MDAs can be fitted like pieces of a jigsaw. This framework is referred to in this document as the E-Government strategy (or E-Strategy).

In implementing the various E-Government programmes, MDAs business processes must be transformed using E-Government technologies.

The E-Government strategy will allow the MDAs to:

- use E-Government to improve productivity by enabling better interactions and coordination
- look beyond current ways of working. (Today's ICT solutions in the MDAs incorporate more productive ways of doing work, either through eliminating paperwork or integrating activities across longstanding organizational silos. MDAs have to introduce document management and workflow systems into their operations, and evaluate ICT systems by considering the internal and external performance benefits they deliver to the programs they support, i.e. how well they respond to citizen's needs rather than how well they serve their internal processes.)
- substantially change current bureaucratic procedures thereby breaking down the inherent resistance to change. This needs a holistic approach to E-

Government, which must be accompanied by results-oriented performance measures, policy alignment, training, communications, and organizational milestones.

Indicative Public Administrative Services

E-Government is expected to facilitate public administrative services to both citizens and the general public. Examples of these services have been enumerated below:

Provided to Citizens

01. Personal income tax; tax relief; tax notices
02. Social security benefits, unemployment benefits, child allowances, health costs, scholarships
03. Birth and death certificates
04. Job search services at the labour office
05. Personal documents (identity cards, passports, driving licenses)
06. Reports to the police (e.g. in case of theft)
07. Address changes
08. Secondary and higher education diplomas
09. Public libraries
10. Education (secondary, tertiary), Examinations
11. Vehicle registration
12. Vehicle insurance
13. Health services
14. Personal insurance

Provided to Businesses

01. Social security for employees
02. Corporate income tax, tax returns and tax notices
03. VAT returns and notices
04. Registration of start-ups
05. Customs declarations
06. Resident permits, work permits, visas
07. Environment related permits
08. Sending of data to the Ghana Statistical Department
09. Weather
10. Public procurement

The Key E-Government Messages

The key messages that the body that will be mandated by law to supervise the implementation of the E-Government initiative (referred to as the E-Government Management Structure in this document) must relay to MDAs and the citizenry at large are that E-Government:

- ***Changes how government works.*** It enables a more networked-style of government, where MDAs act more coherently, making government as a whole easier to deal with. The prerequisites for this transformation are expressed in the reference models and an agreed set of information and technology standards depicted by a component-based architecture discussed in Section 6 of this document. But they also lie in developing shared public sector and civil service data resources, building an infrastructure of shared software and hardware.
- ***Focuses on people***. People want information or services delivered quickly and easily. They are less interested in which part of government provides what. E-government focuses on what gets delivered to people more than on the MDAs that deliver it.
- ***Means better service.*** People's need could be met in a more timely, tailored, and convenient manner while maintaining the privacy and the security of their personal information.
- ***Means better value.*** It enables better use of taxpayers' money because MDAs will share more information and technology, and design improved business processes thereby generating a better return on the public investment involved.
- ***Affects all MDAs.*** Therefore it cannot be ignored. All MDAs deal with the same people who have the same expectations of government.
- ***Collaboration is key to success.*** – E-Government depends on all MDAs working together to deliver results. Therefore all must commit jointly to deliver the results.
- ***Is relevant to all central and local government organizations.*** Therefore all must participate in creating it.
- ***Is about delivering results, not technology*** – it is ***not*** an ICT project. E-Government seeks to deliver results by:
  - managing information better
  - ensuring organisational and cultural changes are enabled by Internet era technologies and business models. Without change, technology will just add to the cost of government without improving the results it delivers.

The Benefits of Implementing E-Government

The benefits of implementing E-Government are oriented towards:

- improving the standard of living of citizens and businesses,
- upgrading the organizational and technological aspects of public sector and civil service administration, and
- improving the technological skills of public sector and civil service administrators.

These benefits have been expanded in the paragraphs below.

Orientation towards citizens and businesses:

E-Government

- Enables wide public electronic access to information,
- Ensures transparency in the activities of the public sector and civil service and offers opportunities for feedback,
- Upgrades the quality of the communication amongst citizens, businesses and government employees through continuous exchange of knowledge, enhancement of the level of competence, and the enhancement of technological and administrative culture,
- Reduces the time, effort and costs needed for integrated public sector and civil services including access to personal and public data, and exchange of electronic documents and other information between citizens, private sector businesses and the public administration,
- Accelerates the process of empowerment and socio-economic development in deprived areas, and the marginalised or under-served – women, illiterate citizens, senior citizens, and the poor – in society.

Orientation towards organizational and technological upgrading of the public sector and civil service administration:

E-Government

- Ensures better interaction among institutions in the public sector.
- Provides a reliable electronic communication infrastructure, which facilitates communications amongst MDAs, the different arms of government (the executive, the judiciary, and parliament), and between government and citizens,

- Provides a reliable national identification and information security system thereby increasing information security and security awareness of government systems. A national identification card could store a digital certificate which will allow users who access E-Government and other services (provided by such institutions as banks, insurance companies, and health providers) to attach an electronic signature which could be used to certify the authenticity of data transmitted,
- Establishes an efficient, effective and integrated Management Information System (MIS) to prevent corrupt practices,
- Provides integrated electronic services to meet the needs of citizens and businesses,
- Enforces the establishment of ICT policies, standards, and quality control systems,
- Enforces the establishment of a sound legal framework to regulate the business processes of E-Government,
- Lowers the overall cost of development and implementation of technology,
- Increases security and security awareness of government systems,
- Mitigates risk when procuring services and technologies,
- Ensures technology is interoperable, robust, scalable, and extensible, supporting expansion and the adoption of industry standards,
- Leverages and propagates existing digital assets across GoG.

Training and retraining of personnel in the public sector and civil service administration:

E-Government

- Provides the necessary human resources for the establishment and operation of E-Government.
- Develops new organizational culture in public sector and civil service administration, ensuring improved quality of services.
- Upgrades the professional, organizational, and managerial skills of public officials.
- Ensures teamwork at the institutional and national levels in order to enhance the quality of management of e-government business processes.

E-Government Opportunities

The opportunities that will be available to MDAs if they embrace E-Government include:

- joint working across and between departments to improve policy development
- standardised format for collection of statistics to inform policy making
- electronic communication between government and parliament
- quicker, cheaper and more efficient public consultation (citizen's panel)
- deploying a cab-e-net system for planning ministerial speeches/ announcements, to avoid overlaps and gaps
- implementing an E-Procurement system at governmental/departmental level to maximise leverage from bulk purchasing power and minimise delays
- implementing cross-departmental accounting systems to support accountability for policy goals
- internal advertisement of vacancies and job applications
- using an online training database for advertising/booking courses
- creating a centralized database to keep, maintain, and update human resource records and payroll data
- creating departmental websites that will have updated information, contact points for enquiries (could use different languages, large type, sound recording)
- making forms available on the Internet
- collecting data electronically, e.g. revenue tax return
- exploiting e-channels for social/economic ends, e.g. public awareness campaigns to encourage immunisation, savings, and so on
- sending and acknowledging receipt of instructions, e.g. court summonses
- enabling citizens to track transaction progress, e.g. with visa application
- transferring information automatically, e.g. one-stop change of address
- providing educational services
- enabling local delivery of services from partnerships, e.g. joint call centres for emergency services, and
- improving claims processing/case management.

Section 5. The E-Government Strategy

This section maps out a strategy for the implementation of E-Government in Ghana. It details a vision for E-Government, objectives, strategic goals, the E-Government Management Structure, an approach for establishing GoG enterprise architecture, and a legal and regulatory framework for E-Government.

Vision

To promote more efficient and effective governance by allowing greater public access to information and services using modern information technologies with the aim of achieving a transparent, accountable, participatory, and easily accessible government.

Objectives

The objectives for the implementation of E-Government are, to:

- provide, through electronic means, high-quality, efficient and accessible public services to citizens, businesses and government
- make government more accountable by making its operations more transparent, thus reducing the opportunities for corruption
- transform the way government interacts with citizens
- provide socio-economic development opportunities by empowering rural and traditionally underserved communities using ICT
- expand the technological capabilities of citizens and businesses for participation in the government decision-making process
- create a government-wide communication and information environment for effective and collaborative functioning of public sector and civil service administration in accordance with internationally acceptable standards and best practices
- streamline bureaucratic and labour-intensive procedures and processes, and
- utilize technology in fostering transparency and empowering people to participate in the political process that affects their lives.

Strategic Goals

The following are the Strategic Goals for the implementation of E-Government:

- ***Strategic Goal 1:*** Establish Institutional Framework to oversee the implementation of E-Government.

- ***Strategic Goal 2:*** Establish a component-based Ghana Government Enterprise Architecture to facilitate efficient and effective citizen to government, government to government, and government to business interaction.

    - ***Sub-Strategic Goal 2.1:***

      Establish Monitoring and Evaluation Mechanisms for measuring the progress of E-Government programmes and MDA operational efficiency and effectiveness.

    - ***Sub-Strategic Goal 2.2:***

      Identify opportunities to simplify processes and unify work across MDAs and within lines of business in government.

    - ***Sub-Strategic Goal 2.3***:

      Identify opportunities to deploy common and specific E-Government Applications and Services across MDAs and within lines of business in government

    - ***Sub-Strategic Goal 2.4***:

      Establish a foundation for the reuse of applications, application capabilities, and components across MDAs, and within lines of business in government.

    - ***Sub-Strategic Goal 2.5:***

      Establish policies, standards, specifications, and technologies that collectively support the secure delivery, exchange and construction of business and application components.

    - ***Sub-Strategic Goal 2.6:***

      Identify the data and information that will support MDA and government operations and establish a repository, which will hold government data (see Appendix D - Metadata).

- ***Strategic Goal 3***: Implement a secure, robust, and interoperable E-Government Infrastructure.

- ***Strategic Goal 4***: Ensure the establishment of a Legal and Regulatory Framework that supports the adoption and implementation of E-Government.
- ***Strategic Goal 5:*** Leverage the use of ICT, within an effective E-Government Environment, to meet vital socio-economic development goals.
- ***Strategic Goal 6***: Seek active and direct participation of the private sector in the implementation of E-Government

These strategic and sub-strategic goals are discussed in detail in the next sections.

Strategic Goal 1: Establish Institutional Framework – The E-Government Management Structure (E-GMS)

A key factor to ensure the successful implementation of E-Government is the adoption of appropriate institutional arrangements that clearly define the roles, functions, and responsibilities, as well as relationships of various stakeholders. There is also the need to adopt corresponding policies that will guide the operation of government institutions and the activities of the private sector in the implementation. Accordingly, and in line with the first strategic goal, the government should:

- establish an E-Government Management Structure, including its secretariat, to review the E-Government strategy, plans and actions and oversee their implementation. The structure will work in collaboration with the proposed Information Technology Services Divisions/Directorates of the MDAs.
- establish the ICT Services Division/Directorate (ITSDs) in all MDA

The E-GMS shall engage in policy advocacy and championship at the highest levels (with the President, members of cabinet, parliament, the judiciary, and local government officials) for the implementation of E-Government.

The E-GMS may be stratified into a **policy-making unit**, and a **technical and implementation unit**. The **policy-making unit** will undertake the following:

- provide leadership, set priorities and recommend strategic directions for implementing E-Government
- review and recommend changes to the E-Government strategy, policies, procedures, regulations and law where appropriate
- ensure that E-Government policy management is carried out at the highest institutional levels to ensure highest levels of authority, responsibility and accountability in the administration of policies and implementation activities
- assist in establishing policies, which shall set the framework for information technology standards for E-Government

- ensure seamless integration of policy, program, technical implementation and management of E-Government

- advise on the resources required to develop and effectively administer E-Government programmes (initiatives) and activities within MDAs

- obtain clear commitments of budgetary support and financing from the relevant stakeholders

- recommend needed legislation on cyber security and appropriate penalties for violators, e-commerce in government, and privacy rights of individuals and companies

- coordinate with the National Security Council, the Bureau of National Investigations, and other related bodies and private sector organizations in establishing a national electronic security and anti-fraud task force emergency response team

- play a central role by coordinating and overseeing the implementation of e-government programmes, initiatives, and activities including:
    - coordinating capital planning, investment control, and funding of E- Government
    - overseeing the appropriate distribution of E-Government funds
    - ensuring the right human resource complement and the right skill mix for the E-Government Organisation
    - ensuring appropriate administration and coordination of the E- Government resources
    - ensuring information security
    - periodically reviewing the Ghana Government Enterprise Architecture
    - ensuring privacy of personal information
    - ensuring access to, dissemination of, preservation of, and confidentiality of government information
    - ensuring accessibility of information technology by underserved and underprivileged communities, and
    - planning, managing, and controlling other areas of e-government
- identify, facilitate, and foster opportunities for public, private, and inter-governmental collaboration in addressing the disparities in access to the Internet and information technology

- sponsor activities to engage the general public in the development and implementation of policies and programs, particularly activities aimed at fulfilling the goal of using the most effective citizen-centered strategies and those activities, which engage multiple MDAs providing similar or related information services and

- perform any other related function assigned by the government.

The **technical and implementation unit,** which shall be sub-coordinated to the policy-making unit, shall:

- develop and maintain the GoG portal
- facilitate the E-Government implementation and provide input for the periodic review and updating of the strategy
- establish standards, guidelines, and mandatory requirements for interconnectivity and interoperability, portals and web guidelines, metadata, operational efficiency, and robust and adaptive information and communication infrastructure
- monitor all ICT infrastructure and respond appropriately to security incidences
- issue all security related advisories
- establish or authorize an institution, or licensing of a private sector firm, to serve as a Certification Authority (CA) for the necessary Public Key Infrastructure (PKI), or any other mechanism for user identification, verification, and authentication to ensure the integrity, security, and legitimacy of all online transactions
- provide the necessary input into the review of the Government of Ghana Enterprise Architecture
- monitor developments in convergent technologies and advise government on the effective application of these technologies
- issue technical advisories to accelerate the conversion of government processes, databases, documents, and transactions into a standardised electronic format
- promote the innovative uses of IT by MDAs & Regional Coordinating Councils (RCCs), and Municipal, Metropolitan and District Assemblies (MMDAs), particularly initiatives involving multi-agency collaboration, through support of pilot projects, research, experimentation, and the use of innovative technologies
- assist MDAs to prepare project proposals, terms of reference, technical and functional specifications, and requests for proposals prior to release to prospective bidders
- liaise with the Ministry of Trade and Industry to promote, coordinate, and negotiate electronic commerce initiatives with foreign governments and inter-government agencies

- identify mechanisms for providing incentives to program managers and other Government employees to develop and implement innovative uses of IT

- ensure effective implementation of electronic procurement initiatives by MDAs

- ensure compliance with budgetary and budget implementation standard through the Medium Term Expenditure Framework (MTEF) review process

- measure, monitor, and evaluate the progress of E-Government implementation progress, and

- ensure that electronic government activities incorporate adequate, risk-based, and cost-effective measures.

It will also be necessary for the Government of Ghana to make it a requirement for all MDAs to have a Chief Information Officer (CIO), or somebody with a similar designation, who will be responsible for implementing E-Government programmes and initiatives in the organization. The head of the E-GMS may also be designated as a government CIO.

Judging from international experience, the CIO will have to be multi-skilled in the following areas:

- ICT strategy
- ICT resource management
- business strategy (especially strategic intelligence)
- public sector policy, practices, procedures, and processes
- political sensitivity
- advocacy
- organizational governance and leadership
- communication skills
- change management
- project management
- risk management
- customer relationship management
- organization development, and
- ICT research and development.

Since it is rare to find a single individual who has a combination of these skills, and since the country will require many of such individuals going forward, it will be

imperative to follow international best practice by making a tertiary or management development institution design and deliver a course to cater for this need. It will also be necessary for the other staff who will be working with these CIOs to be trained in various ICT disciplines. People occupying positions just below the CIO will also have to undergo project management, change management, and risk management training. Once these people have been trained, it will be necessary to cascade the skills acquired to the levels below them via seminars and workshops.

Strategic Goal 2: Establish a Component-Based Ghana Government Enterprise Architecture

The **Ghana Government Enterprise Architecture (GGEA),** adopted from the Federal Enterprise Architecture of the United States of America, is depicted on the next page. It provides a government-wide business-based framework, which will allow MDAs in Ghana share and leverage common data, information, and business functions across the entire government. The architecture is a collection of interrelated **"reference models"** designed to facilitate cross-MDA analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across MDAs. The architecture describes how the government performs its work using people, business processes, data, and technology. It will reinforce E-Government's drive towards more homogenous information and technology environment characterised by:

- collaborating and sharing
- focusing on leveraging maximum value
- increasing standardisation of data, information systems and business processes, and
- developing a new governance arrangement at the governmental level (a whole-of-government level - this should be taken out unless it is a term).

As Figure 2 on the next page depicts, the reference models are, the:

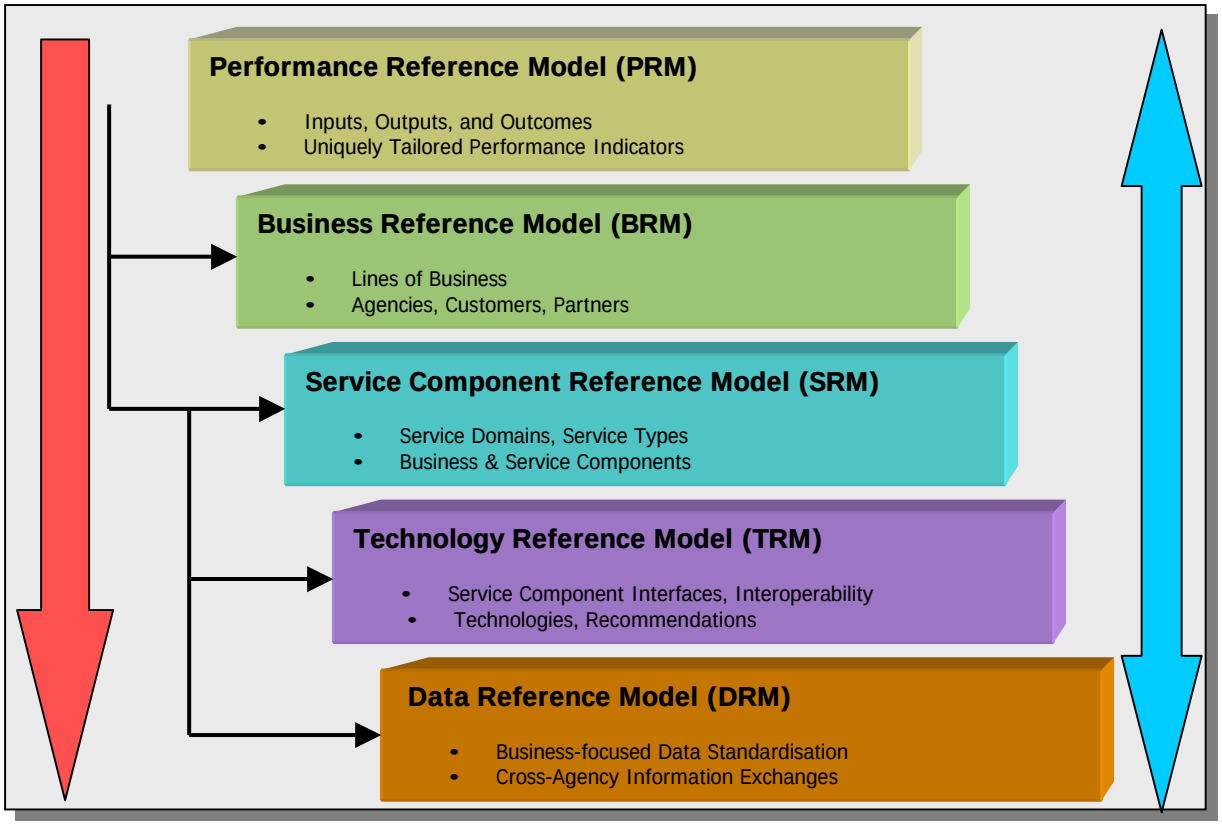
- Performance Reference Model (PRM)
- Business Reference Model (BRM)
- Service Component Reference Model (SRM)
- Technology Reference Model (TRM), and
- Data Reference Model (DRM)

The reference model approach facilitates the communication of architectural ideas within and across MDAs.

The government-wide Enterprise Architecture (EA) has integrated, citizen-centric processes that will facilitate the elimination of investments in redundant ICT capabilities, business processes, or other capital assets. Furthermore, the model will aid in the identification of common business functions across MDAs, and in the

integration of performance measurement with the budget process along the key government lines of business.

Figure 2: The 5 Reference Models



Establishing the EA will also ensure the ability of MDAs to:

- save time and money by leveraging re-usable business processes, data, and ICT components in other MDAs
- leverage EA work products as a catalyst for MDAs-specific EA efforts, and
- ensure proposed investments of a particular MDA are not duplicated with those of other MDAs

Application of the EA will yield a wealth of information on government business lines, programmes, and capital investments. This information could be made available to parliament as it considers the authorization and appropriation of funding for government programmes, and as it fulfills its oversight responsibilities on behalf of the citizen.

The various reference models are discussed in detail in the sub-sections below.

Sub-Strategic Goal 2.1 **- Establish Monitoring and Evaluation Mechanisms for measuring the progress of E-Government programmes, and MDA operational efficiency and effectiveness. (The Performance Reference Model)**

The **Performance Reference Model** is a standard framework to measure performance of major ICT initiatives and their contribution to program performance. The model provides common outcome and output measures throughout government allowing MDAs to better manage the business of government at a strategic level while providing a means for gauging progress towards the target EA. The PRM accomplishes these goals by establishing a common set of general performance outputs and measures that MDAs shall use to achieve much broader program and business goals and objectives.

The standardized framework has three main purposes:

- help produce enhanced ICT performance information to improve strategic and daily decision-making
- improve the alignment – and better articulate the contribution of – ICT to business outputs and outcomes, thereby creating a clear **"line of sight"** to desired results, and
- identify performance improvement opportunities that span traditional organizational structures and boundaries.

The model, depicted as Figure 3 on the next page, articulates the linkage between internal business components and the achievement of business and customer-centric outcomes. Most importantly, it facilitates resource allocation-decisions based on comparative determinations of which programs/organizations are more efficient and effective.

The PRM is structured around:

- **Measurement Areas:** the high-level organizing framework of the PRM that captures aspects of performance at the input, output, and outcome levels. As depicted on the diagram on the next page, the PRM comprises six (6) measurement areas:
    - ***Mission and Business Results*** driven by the Business Reference Model (defined further on in this section) to ensure that outcomes are appropriately aligned to what MDAs do
    - ***Customer Results*** capture how well an MDA or specific process within an MDA is serving its many customers spanning the citizen, business, other government, and internal categories
    - ***Processes and Activities*** driven by the Mode of Delivery Business Area of the BRM and it captures the outputs that are the direct result of the process that an ICT initiative supports
    - ***Human Capital***
    - ***Technology*** designed to capture key elements of performance that directly relate to an ICT initiative, and
    - ***Other Fixed Assets***

Figure 3: The Performance Reference Model

- **Measurement Categories:** groupings within each Measurement Area that describe the attribute or characteristics to be measured. For example, the Mission and Business Results Measurement Area has three (3) categories:
    - Services to Citizens
    - Support Delivery of Services, and
    - Management of Government Resources
- **Measurement Indicators:** generic indicators that MDAs are free to tailor to fit their specific environment and the ICT initiative's specific goals.

The PRM structure is designed to clearly articulate the cause-and-effect relationship between inputs, outputs, and outcomes. Though this relationship is rarely direct cause-and-effect, the PRM structure seeks to "tease out" the contribution an ICT initiative makes to improved process and business performance (which when measured may only be a mere association).

The "line of sight" is critical for ICT project managers, program managers, and key decision-makers to understand how and to what extent technology is enabling progress towards outputs and outcomes. The PRM captures this "line of sight" to reflect how value is created as inputs (such as Technology) are used to help create outputs (through Processes and Activities), which in turn impact outcomes (such as Mission and Business).

The PRM's true value is synergistic and comes not from each individual Measurement Area, but when multiple Measurement Areas are used together to understand the full value and contribution of an ICT initiative.

Specifically, effective use of the PRM requires identification of a critical few Operationalised Measurement Indicators in each of the relevant Measurement Areas to draw the "line of sight" from the ICT initiative to the processes and activities it supports—and by extension the customer results and mission and business results it enables. Though the PRM includes many indicators, its value is not in the sheer number of indicators it includes. Rather, its value is realized when used to identify a critical few indicators that can provide information for decision-making.

The E-GMS will have to establish an Annual ICT Performance Review of MDAs E-Government plans, programmes, and actions.

Sub-Strategic Goal 2.2 **- Identify opportunities to simplify processes and unify work across MDAs and within lines of business in government. (The Business Reference Model)**

To be able to identify opportunities which will simplify processes and unify work across MDAs and within the lines of business of the government, it is necessary for government to establish a **Business Reference Model (BRM)** depicted as Figure 4 on the next page.

It separates government operations into four main business areas, the

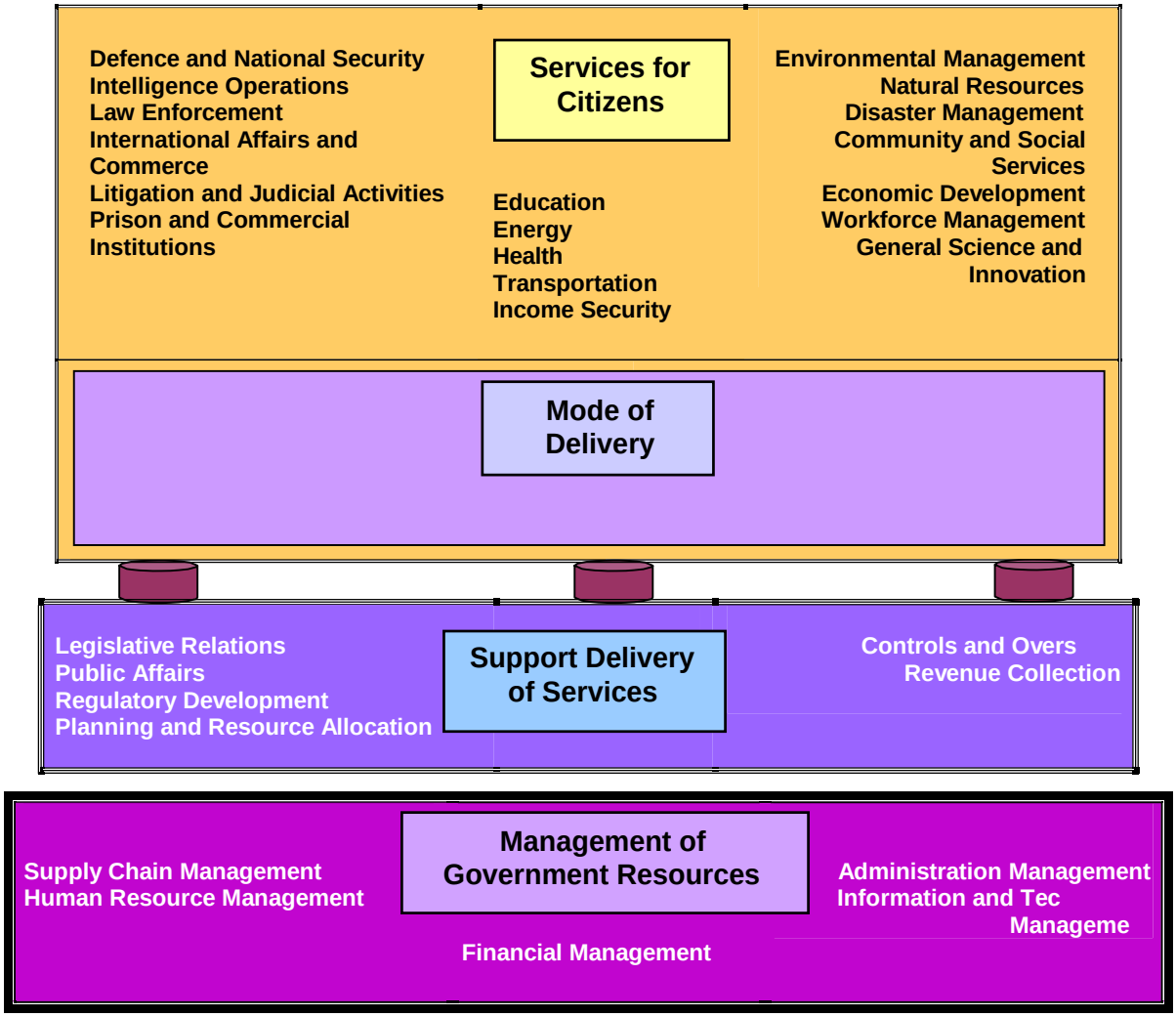
- Services for Citizens business area
- Mode of Delivery business area
- Support Delivery of Services business area, and
- Management of Government Resources business area.

The BRM is a functional-driven framework for describing the business operations of government independent of the MDAs that perform them.

The ***Services to Citizens*** Business Area includes the delivery of citizen-focused, public, and collective goods and/or benefits as a service and/or obligation of the Government of Ghana to the benefit and protection of the nation's general population.

The ***Support Delivery of Services*** Business Area provides the critical policy, programmatic and managerial underpinnings that facilitate the government's delivery of services to citizens and other state and local MDAs.

Figure 4 : The Business Reference Model

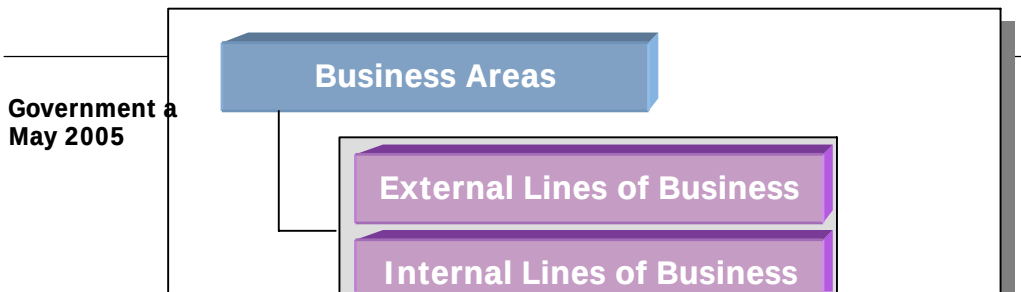


The ***Mode of Delivery*** Business Area describes the mechanisms the government uses to achieve the purpose of government, or its Services for Citizens. It includes two main categories – Financial Vehicles and Government Service Delivery.

The ***Management of Government Resources*** Business Area refers to the "back office" support activities that must be performed for the government to operate effectively.

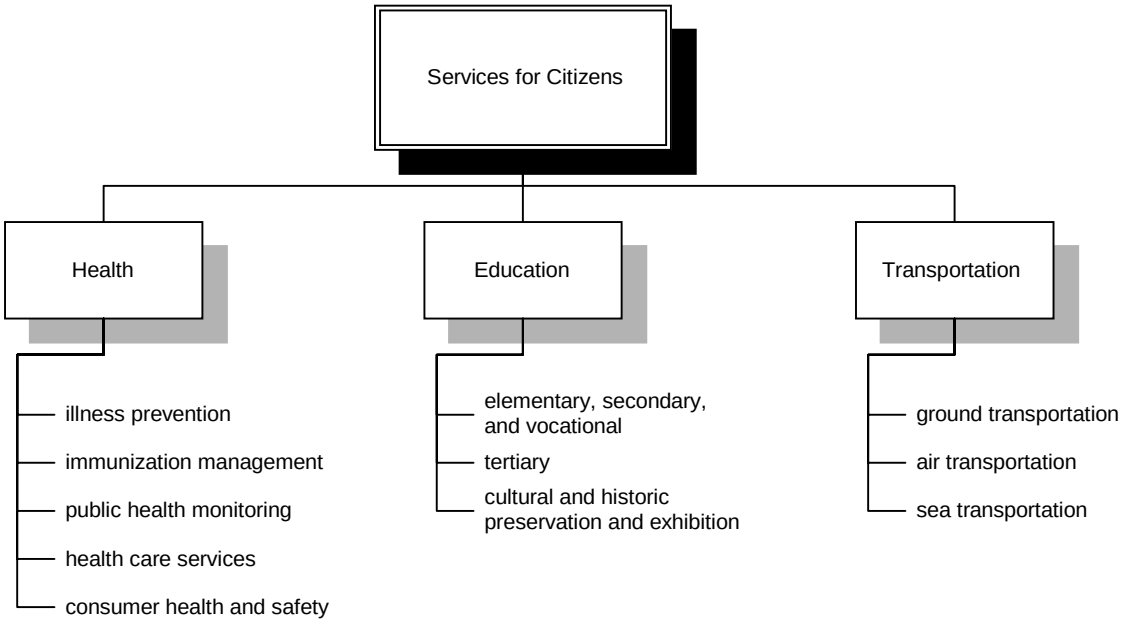
The model provides a common understanding of the entire government business for MDAs, oversight bodies, ICT decision makers, business partners, vendors, and even citizens. It provides a hierarchical construct (see Figure 5 below) for describing the day-to-day business operations of the government.

Figure 5: The Hierarchical Relationship of the BRM Components



The business area box in this three-tiered construct refers to the four (4) business areas defined in the previous diagram. Each of these four business areas is divided into internal and external lines of businesses. Each line of business is divided further into sub-functions. Figure 6 below illustrates this concept with education, health, and transportation as examples.

Figure 6: Education, Health, and Transportation



The purpose of the BRM is to define and communicate, for all interested stakeholders, a high-level view of how – in business terms – the government achieves its various missions. It enables users to identify how processes are being supported, where there are opportunities to reduce redundancies, and how to build more cost-effective solutions in the future.

The BRM will provide a common reference point and a foundation for improvement in a variety of key areas, such as:

- performance measurement
- budget allocation
- information technology redundancy elimination, and
- cross-MDA collaboration

The functional perspective of the BRM facilitates identification of common business processes, information requirements, and opportunities for reengineering across government rather than within the confines of organizational stovepipes. It is an analytical tool that provides a detailed process map to help MDAs to identify processes, programs, and systems that can be made more efficient through cross-MDA collaboration. The BRM serves as a foundation from which the other layers of the EA can be developed.

When considering transforming services in the ***Management of Government Resources*** Business Area, it will be pertinent for GoG to consider adopting the shared service approach. With this approach, GoG can pull the non-strategic

activities which support core business processes out of each business unit and consolidate them into a separate (stand-alone) operating unit (or organization) that will run these supporting processes as its core business process in order to achieve critical mass. The business units can then be freed up to manage their strategic goals. Freeing up the business unit this way allows its management to focus on solving business problems by enhancing the business unit's core processes, thus enhancing the value chain and in turn enhancing growth. Government shared services are beneficial because they:

- enhance government's corporate value
- allow government's business units to focus on the strategic aspects of operations
- transfers what business units consider as secondary activities into core process of the shared services thereby affording these services the necessary care that they merit
- focus on service and support to the business units who become "business partners" of the shared service unit
- increase productivity by doing more with less
- provide concentration of resources that perform the same support activities
- provide supporting activities at lower cost with higher service levels
- leverage technological investments
- leverage purchasing by consolidating vendors in order to negotiate better terms and prices
- consolidate transactions of common customers and vendors who deal with more than one business unit. This provides for economies of scale, standardization of process and experiences as they pertain to these customers/vendors
- create working-capital improvements from standardizing, concentrating, and netting treasury activities, as well as from operating receivables, payables, and inventory management in a centre of expertise. This creates economies of scale and improves span of control, and thus, decreases expenses
- create new management responsibility, and
- focus on continuous improvement.

Sub-Strategic Goals 2.3 **- Identify opportunities to deploy common and specific E-Government Applications and Services across MDAs and within lines of business in government.**

Sub-Strategic Goals 2.4 **- Establish a foundation for the re-use of applications, their capabilities, and components across MDAs and within lines of business in government.**

(The Service Component Reference Model)

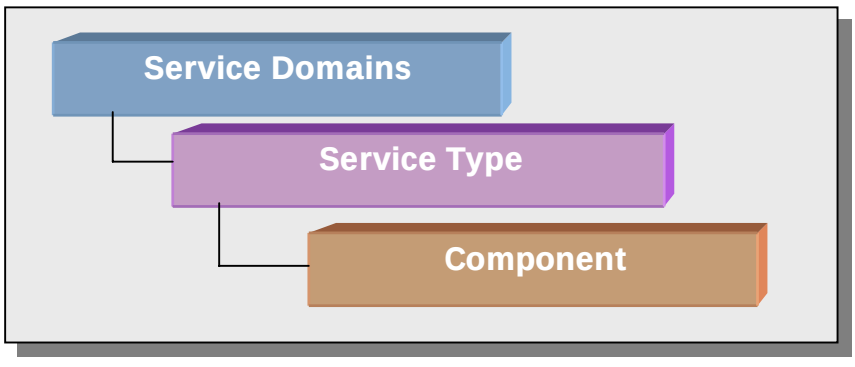
The SRM is a component-based framework that can provide – independent of business function– a leverage-able foundation for re-use of applications, application capabilities, components, and business services. A component is *"a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface."*

The SRM serves to identify and classify horizontal and vertical service components that support MDAs and their ICT investments and assets. The model will aid in recommending service capabilities to support the reuse of business components and services across the government. Specifically, the SRM:

- provides a framework that identifies service components and their relationships to the technology architecture of MDAs across government
- classifies, categorizes and recommends components for the re-use of business services and capabilities across government
- defines existing service components that may be leveraged outside MDA boundaries, and
- is expected to evolve based on new services and components as they are discovered across industry and markets.

The Service Component Reference Model is organised as a functional hierarchy, shown as Figure 7 below, with *Service Domains* at the highest level followed by *Service Types* and *Components*.

Figure 7: The Hierarchical Relationship of the Service Component Reference Model

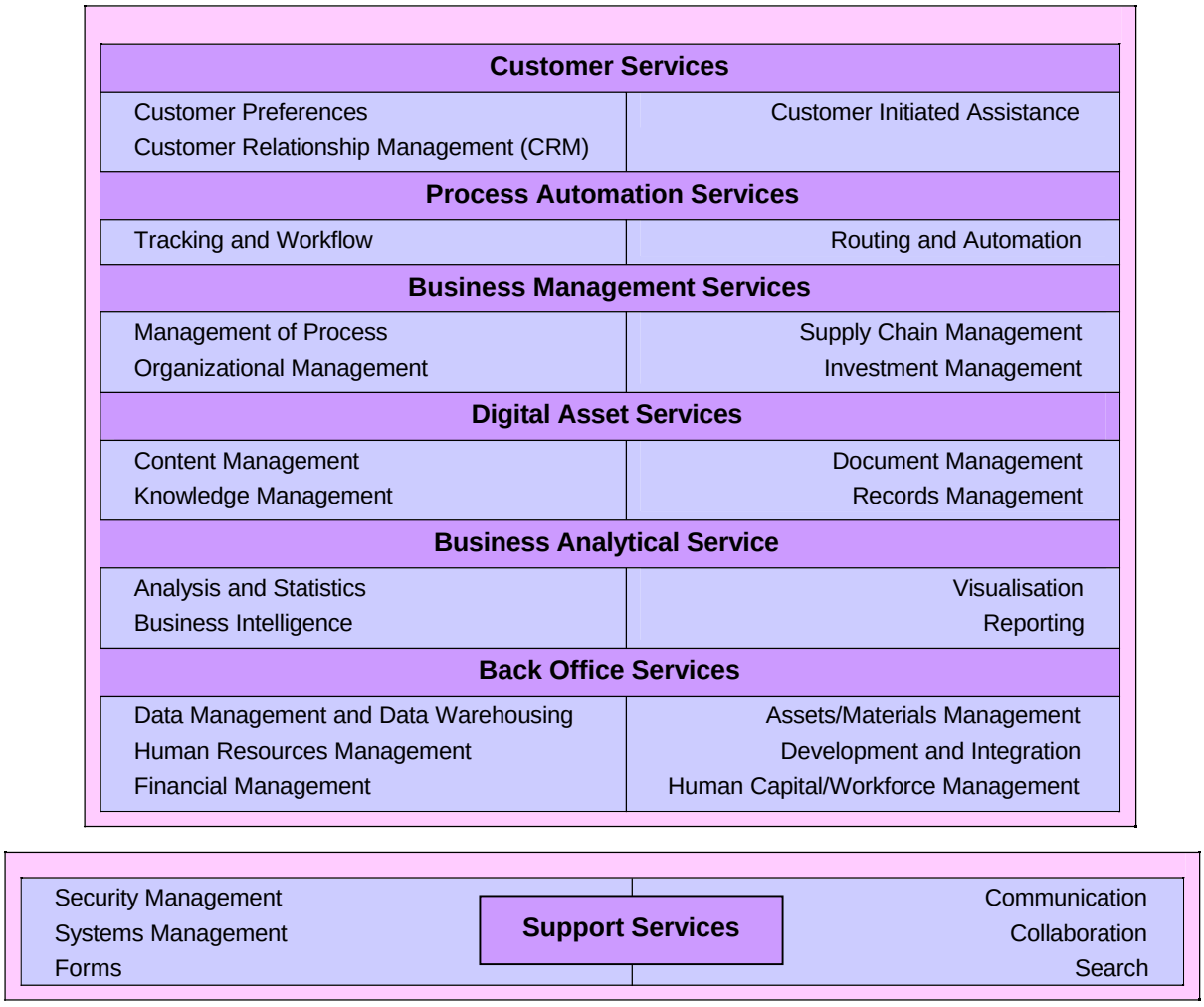


There are 7 Service Domains that provide a top-level categorization of the service capabilities and categories from a business perspective. These Service Domains are, the:

- Customer Services
- Process Automation Services
- Business Management Services
- Digital Access Services
- Business Analytical Services
- Back Office Services, and
- Support Services

These are shown in Figure 8 below.

Figure 8: The Service Component Reference Model



These seven Service Domains are comprised of Service Types as depicted in Figure 8, which further categorizes and defines the capabilities of a Service Domain defining the second level of detail that describes a business-oriented service. The next and final layer of the SRM is the Component level. The Service Domains are discussed in the next few paragraphs.

The Customer Services Domain

The Customer Services Domain defines the set of capabilities that are directly related to an internal or external customer, the business interaction with the customer, and the customer-driven activities or functions. The Customer Services domain represents those capabilities and services that are at the front end of a business, and interface at varying levels with the customer.

The Process Automation Services Domain

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

Business Management Services Domain

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

Digital Asset Services

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

Business Analytical Services

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

Back Office Services

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

Support Services

The Support Services Domain defines the set of cross-functional capabilities that can be leveraged independent of Service Domain objective and/or mission. The Service Types and Components of these Domains have been provided in Appendix G of this Document.

Sub-Strategic Goal 2.5 **- Establish policies, standards, specifications, and technologies that collectively support the secure delivery, exchange and construction of business and application components.**

The Technical Reference Model

The Technical Reference Model (TRM) outlines the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (service components) that may be used and leveraged in a Component-Based or Service-Orientated Architecture. It provides a foundation to advance the re-use of technology and component services. The TRM identifies the core technologies that support the government's ICT transition towards interoperable E-Government solutions. The TRM comprises four (4) core Service Areas as depicted in Figure 9 on the next page.

The Service Areas represent a technical tier supporting the secure construction, exchange, and delivery of Service Components. Each Service Area aggregates and groups the standards, specifications, and technologies into lower-level functional areas. The four (4) Service Areas within the TRM are described as follows:

Service Access and Delivery - refers to the collection of standards and specifications to support external access, exchange, and delivery of Service Components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific Service Component.

Service Platform and Infrastructure - refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities.

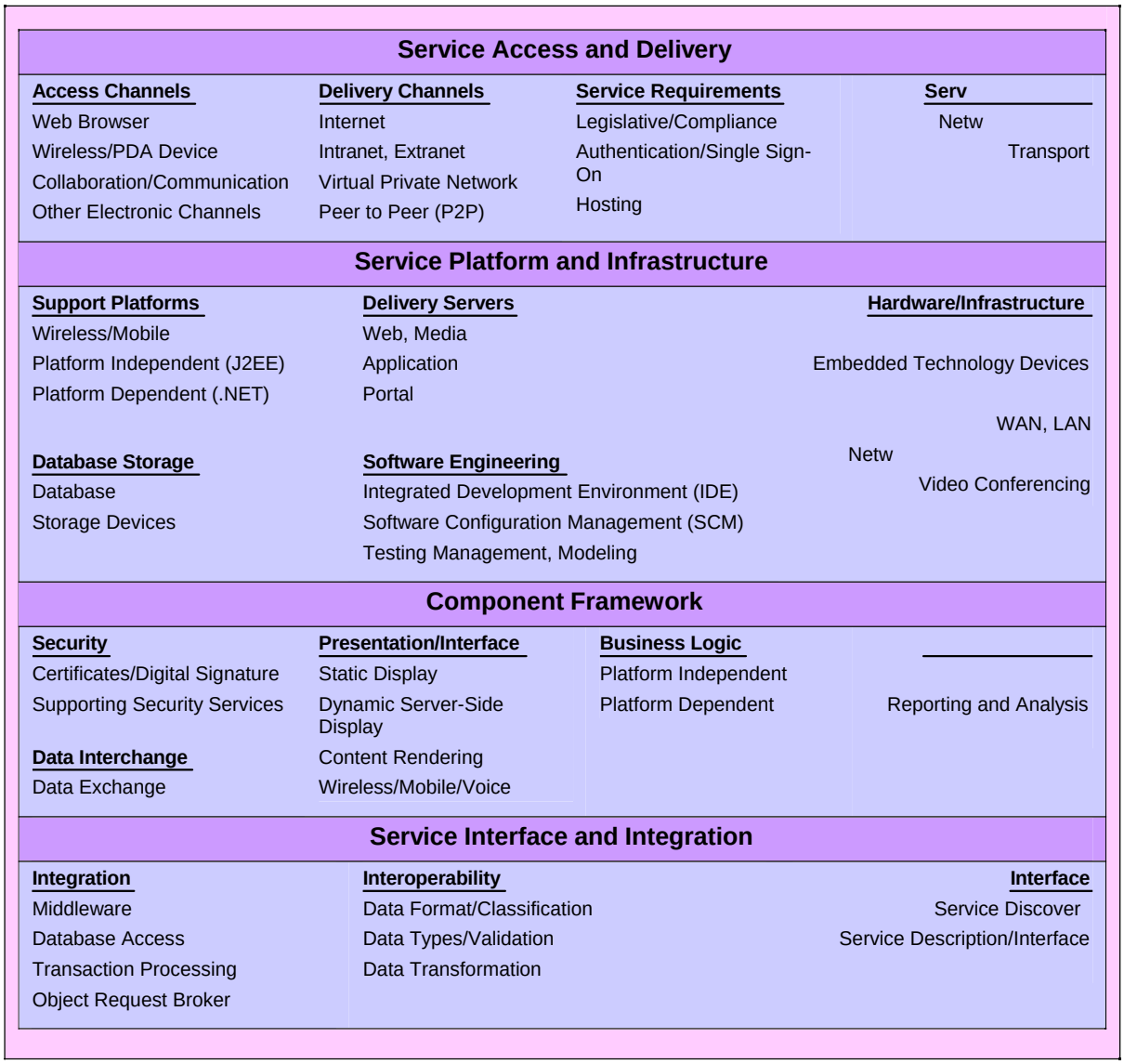
Component Framework - refers to the underlying foundation, technologies, standards, and specifications by which Service Components are built, exchanged, and deployed across Component-Based, Distributed, or Service-Orientated Architectures.

Service Interface and Integration - refers to the collection of technologies, methodologies, standards, and specifications that govern how MDAs will interface (both internally and externally) with a Service Component. This area also defines the methods by which components will interface and integrate with back office/legacy assets.

Supporting each Service Area is a collection of Service Categories. Service Categories are used to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve. Each Service Category is supported by one or more Service Standards.

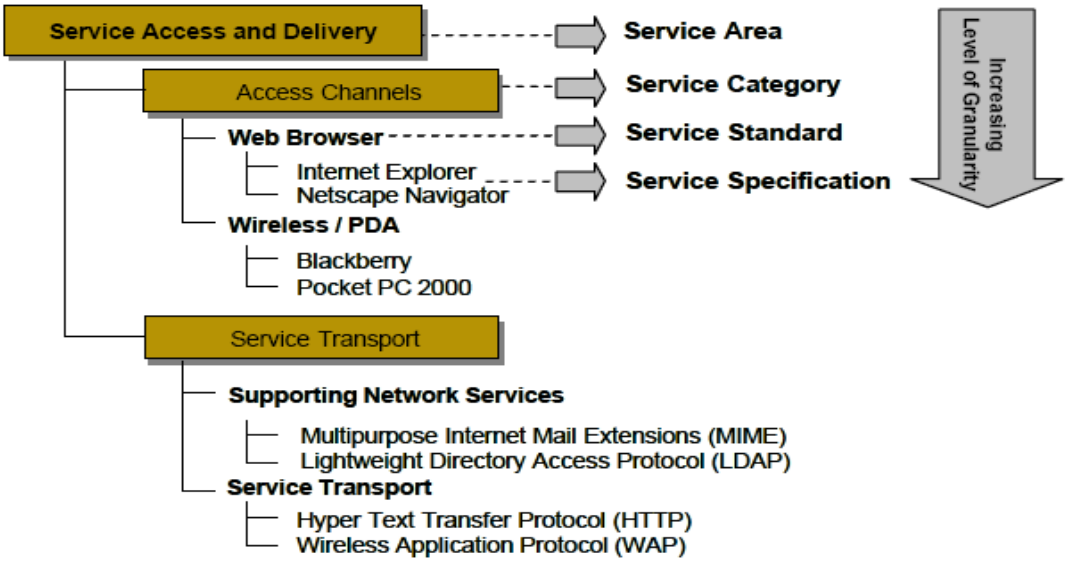
Service Standards are used to define the standards and technologies that support the Service Category.

Figure 9: The Technical Reference Model



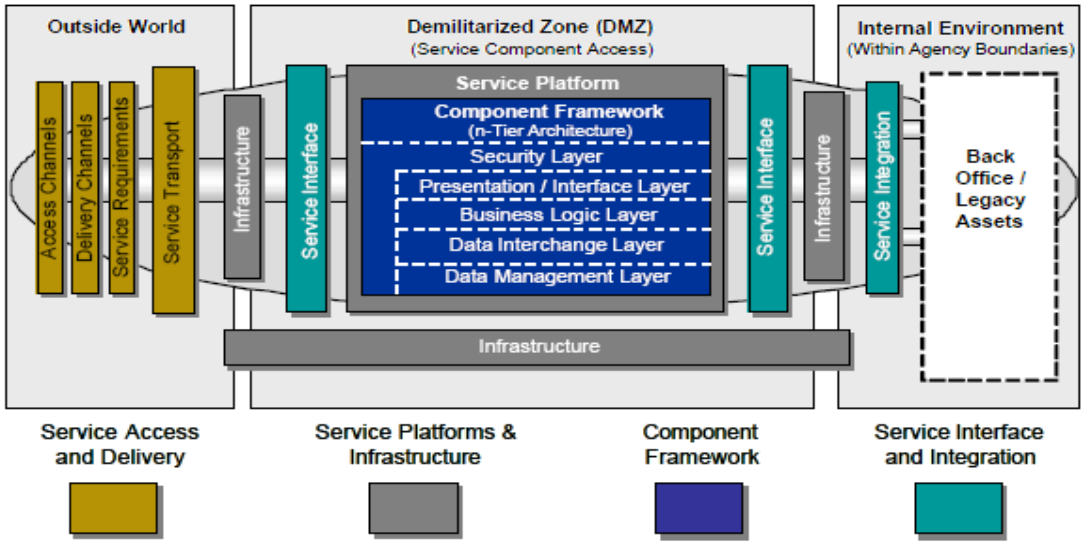
The final level of the TRM is the Service Specification layer that details the specification and/or provider of the Service Standard specification. This concept has been visually represented in Figure 10 below.

Figure 10: The Hierarchical Relationships of the Technical Reference Model



As depicted in Figure 11 on the next page, each Service Area and supporting Service Categories can be structured across typical network topologies that provide clear distinctions between the External and Internal Environments, and the Demilitarized Zones (transitional areas) in between the two. The TRM should aid in the establishment of a framework for Interoperability, guidelines for constructing MDA Websites, and standards for a secure electronic environment

Figure 11: Structuring Service Areas and Service Categories Across a Network Topology



Sub Strategic Goal 2.6 **- Identify the data and information that will support the MDA and government operations and establish a repository which will hold data about government data. (The Data and Information Reference Model)**

The **Data and Information Reference Model (DRM)** will describe, at an aggregate level, the data and information that support program and business line operations. The model will:

- aid in describing the types of interactions and information exchanges that occur between the government and its various customers, constituencies, and business partners
- categorise government's information along general content areas into greater levels of detail
- establish a commonly understood classification for government data leading to identification of duplicate data, and
- streamline the processes associated with information exchange both within government and between the government and its external stakeholders.

The DRM has to be produced on a business line by business line basis, as opposed to a single cumulative effort. This will allow for the identification and concentration of key improvement areas, producing clearly identified and measurable results. The E-Government Management Structure has to carefully and religiously oversee the focused DRM efforts to ensure all appropriate points of integration are identified. It is expected that the DRM will facilitate the establishment of a Metadata Standard.

Making the EA Work

All MDAs need to collaborate to make the architecture work. They need to:

- work with the E-GMS to understand and develop the architecture, and
    - bring their own ICT environments into alignment with it, and
    - design service delivery process that make use of the architecture
- participate in the ongoing design and governance of the architecture
- collaborate with each other in the development and use of access channels, and sharing of back office information and business delivery systems
- contribute to the all-of-government parts of the architecture (e.g. creating metadata; designing, developing, and sharing modular components), and
- use collective governance arrangements to share some decision-making around their information and technology environments to meet whole-of-government objectives.

The E-GMS needs to:

- develop and operate some of the common and modular components of the architecture
- work with MDAs to design governance structures appropriate to the various components of the architecture
- assist MDAs to develop access and delivery channels, and back-office systems collaboratively, and
- explore the possibility of rationalising and consolidating government ICT infrastructure, applications and data to deliver better quality services and better use of taxpayer's funds.

Component-Based Architecture

To help MDAs implement E-Government, government must create a **Component-Based Architecture (CBA)** that outlines a set of recommendations encompassing the selection of tools, technologies, best practices, and standards that should be considered when implementing new systems and/or components to support the selected initiatives.

A CBA should support common component development from an all-of-government perspective, component re-use ('develop once, use many times'), component distribution among MDAs, and cross-MDA collaboration. In areas of technology, MDAs will be faced with difficult decisions regarding

- which technologies to choose
- which standards to support
- what strategies to use to support cross-MDA collaboration
- how to effectively exchange data, and
- how to ensure today's technology will support tomorrow's business objectives.

For these reasons, deploying a Component-Based Architecture becomes a valuable resource which helps to mitigate risks.

Many aspects of services provided by MDAs are generic (e.g. 'accept an electronic payment', 'authenticate an individual', 'change address', 'deliver a secure e-mail') and are therefore best done in a standardised manner by all MDAs using a CBA. A CBA therefore embraces:

- ***common components:*** components developed and implemented only once, and used by many or all MDAs
- ***modular components:*** standard components that support a generic activity ('on-line registration'), but are implemented locally, and

- ***unique components:*** components that are specific to a particular MDA, function, or service.

To ensure successful implementation of a governmental enterprise architecture that is based on a Component-Based Architecture, government has to establish an E-GMS, a body that will work with MDAs to develop and pilot a new approach to developing and using technology across the public sector. This approach will augment MDA-specific application development by developing modular re-usable technology components. Examples of such technology include:

- web-based search tools
- shared workspaces
- mailing list applications
- workflow tools for inter-MDA shared business processes, and
- all-of-government news syndication

The architecture will be at the heart of the E-Government strategy, and it is therefore imperative that all MDAs take part in creating a business and ICT environment based on this architecture.

Deploying a CBA will create an array of short- and long-term benefits for MDAs, the public, and others who will interact electronically with government including:

- assurance that systems and initiatives will align to common standards, and
- prioritisation of critical business systems across government.

GoG must therefore define, develop, deploy, and govern a Component-Based Architecture that encompasses industry standards, best practices, proven technologies, and a forward-thinking foundation that supports and enables MDAs to reap the benefits outlined in Section 4 of this document.

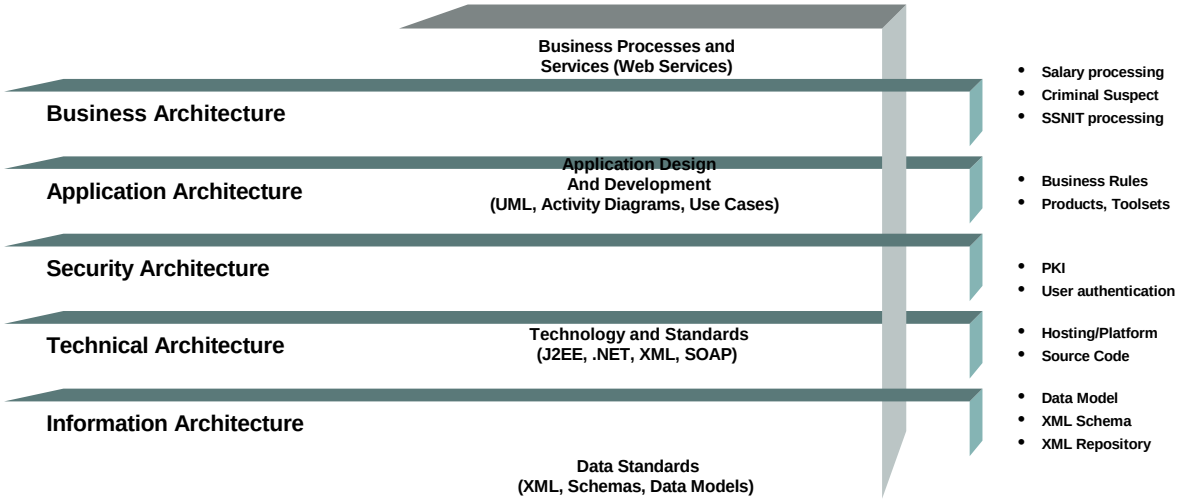
A baseline CBA model should include policies, guidance, and recommendations that outline:

- Stakeholder Collaboration
- Component Definition
- Architecture Standards
- Security Standards
- Industry Standards
- Platform Standards

Stakeholder Collaboration

Working in close collaboration with MDAs, there will be the need to seek avenues in which MDAs can leverage a government-wide strategic framework to ensure that the adoption of technologies and standards are driven from a business/government stakeholder perspective. For example, there could be a definition for a high-level strategy to support the use and implementation of XML across MDAs. An **Integrated Component-Based Architecture Model** is depicted below

Figure 12: The Integrated Component-Based Architecture



Using an "Import and Export" example, if there is a need to provide the name and address of an exporter to multiple systems at different MDAs (e.g. CEPS, GEPC), an inter-MDA name and address XML schema could be used to allow data sharing among the different systems.

The XML schema is one example of the many components that may be necessary to perform a certain task, such as exporting goods.

In this example, the component will facilitate name and address data sharing by the use of open standards and industry-proven technologies, reducing the need of proprietary software while maximizing the potential of re-use.

Business Architecture

The Business Architecture layer of the CBA maps onto the **Business Reference Model (BRM)** and the **Performance Reference Model (PRM)**.

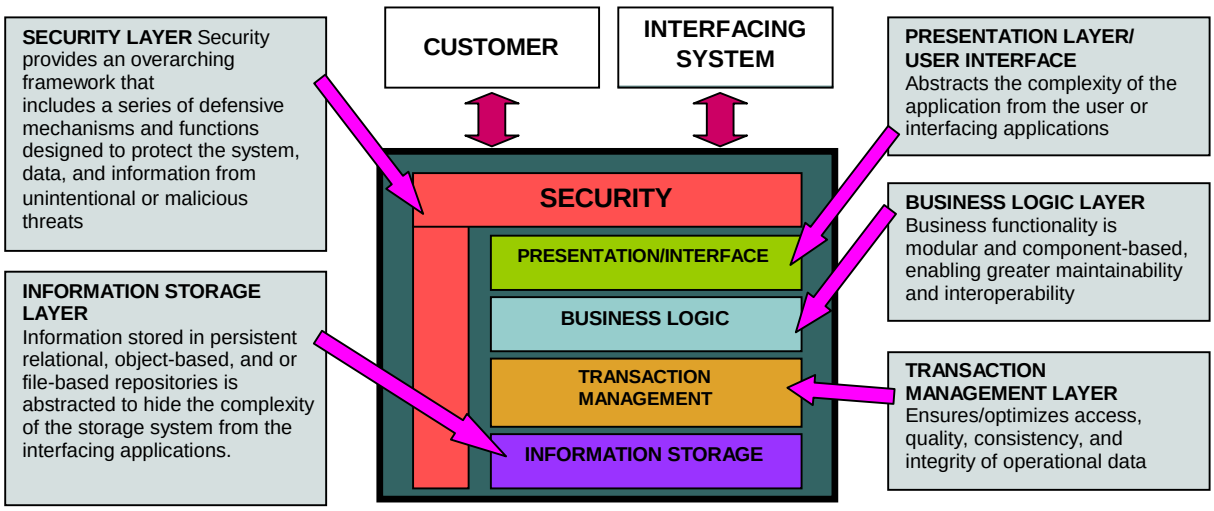
Application Architecture Standards

The reference model for this layer of the CBA is the **Service Component Reference Model.** This reference model deals with such application areas as knowledge

management, customer relationship management, content management, collaboration, reporting, and search capabilities.

The applications ought to be built using the architecture depicted in Figure 13 below.

Figure 13: Applications Architecture



Because the layers have been partitioned, developers can create components using a "building block" approach aimed at reuse and interoperability. Using this approach, MDAs will reduce solutions and the components development costs while increasing the speed in which they can be developed.

Security Standards

In implementing recommended controls to mitigate risk, every MDA should consider a combination of **management, operational,** and **technical** security control standards to maximize the effectiveness of controls for their ICT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to an MDA's mission.

Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an MDA's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards, which are carried out through operational procedures to fulfill the MDA's goals and missions.

An MDA's security standard should establish a set of controls and guidelines to ensure that security procedures governing the use of the MDA's ICT assets and resources are properly enforced and implemented in accordance with the MDA's goals and mission. Management plays a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls.

Operational controls, implemented in accordance with a base set of requirements (e.g., technical controls) and good industry practices, are used to correct operational

deficiencies that could be exercised by potential threat-sources. To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing operational controls must be clearly defined, documented, and maintained.

Technical security controls can be configured to protect against given types of threats. These controls may range from simple to complex measures and usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware. All of these measures should work together to secure critical and sensitive data, information, and ICT system functions.

Technical controls can be grouped into the following major categories, according to primary purpose:

- **Support:** Supporting controls are generic and underlie most IT security capabilities. These controls must be in place in order to implement other controls.
- **Prevent:** Preventive controls focus on preventing security breaches from occurring in the first place.
- **Detect and Recover:** These controls focus on detecting and recovering from a security breach.

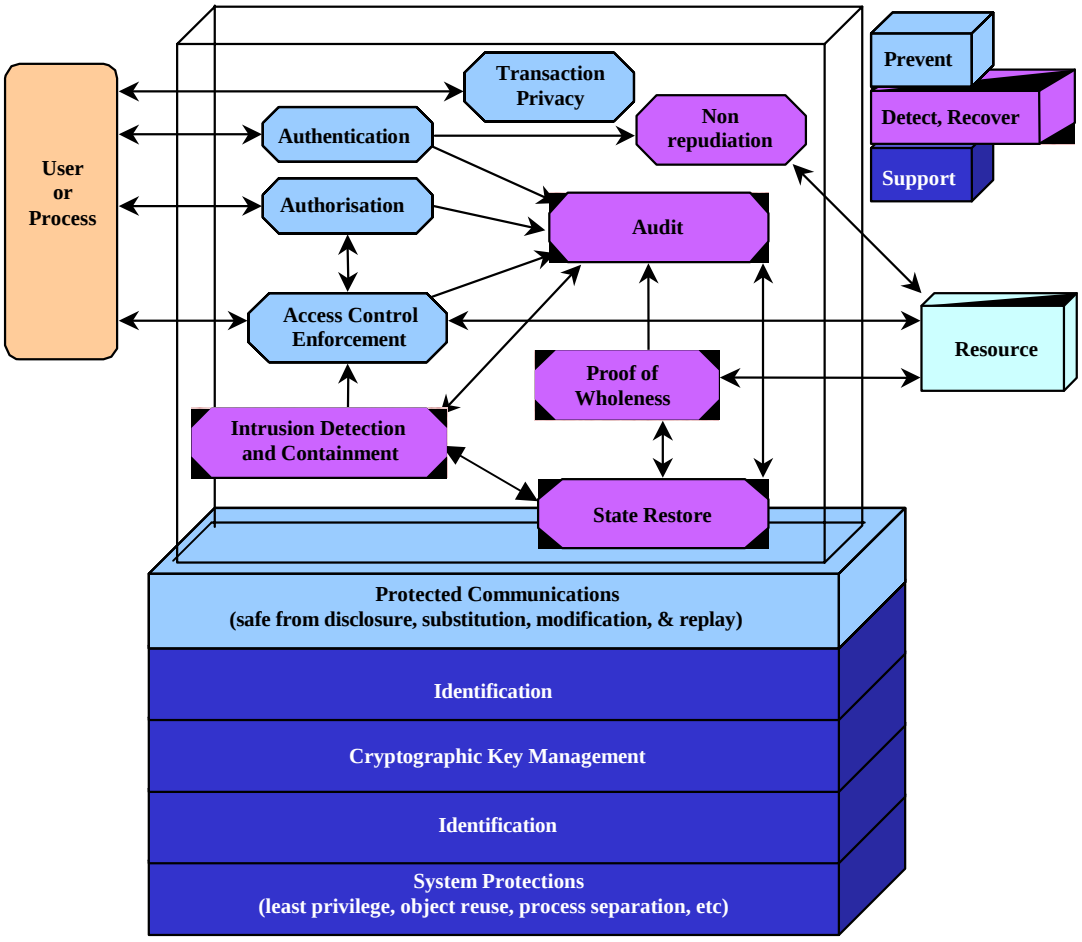
Figure 14 on the next page depicts the primary technical controls and the relationships between them.

Supporting Technical Controls

Supporting controls are, by their very nature, pervasive and interrelated with many other controls. The supporting controls are as follows:

- **Identification:** Identification is the creation of a unique identifier for each user and each system. This control provides the ability to uniquely identify users, processes, and information resources. To implement other security controls (e.g., discretionary access control [DAC], mandatory access control [MAC], accountability), it is essential that both subjects and objects be identifiable.
- **Cryptographic Key Management:** Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. Cryptographic key management includes key generation, distribution, storage, and maintenance.

Figure 14: Technical Security Controls and the Relationships Between Them



- **Security Administration:** The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment. System security can be built into operating system security or the application. Commercial off-the-shelf add-on security products are available.
- **System Protections:** Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object re-use), least privilege (or "need to know"), process separation, modularity, layering, and minimization of what needs to be trusted.

Preventive Technical Controls

These controls, which can inhibit attempts to violate security policy, include the following:

- **Authentication:** This is the process of verifying that a user or entity requesting access to data or a computer resource is who or what it claims to be. The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid. Authentication mechanisms include passwords, personal identification numbers, or PINs, and emerging authentication technology that provides strong authentication (e.g., token, smart card, digital certificate, Kerberos).
- **Authorization:** Authorization is the process of granting or denying rights to an authenticated user or entity to access, read, modify, or delete certain data or to execute certain programs. The authorization control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users).
- **Access Control Enforcement:** Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy (e.g., MAC or DAC). These policy-based controls are enforced via access control mechanisms distributed throughout the system (e.g., MAC sensitivity labels; DAC file permission sets, access control lists, roles, user profiles). The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).
- **Non-repudiation:** Non-repudiation protects against a sender/recipient of data denying that data, or acknowledgement, was sent. System accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Non-repudiation spans both prevention and detection. It has been placed in the prevention category in this guide because the mechanisms implemented prevent the successful repudiation of an action (e.g., the digital certificate that contains the owner's private key is known only to the owner). As a result, this control is typically applied at the point of transmission or reception.
- **Protected Communications:** In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network, Internet Protocol Security [IPSEC] Protocol), and deployment of cryptographic technologies (e.g., Data Encryption Standard [DES], Triple DES, RAS, MD4, MD5, secure hash standard, and escrowed encryption

algorithms such as Clipper) to minimize network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.

- **Transaction Privacy:** Both government and private sector systems are increasingly required to maintain the privacy of individuals. Transaction privacy controls (e.g., Secure Sockets Layer, secure shell) protect against loss of privacy with respect to transactions performed by an individual.

Detection and Recovery Technical Controls

Detection controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. Recovery controls can be used to restore lost computing resources. They are needed as a complement to the supporting and preventive technical measures, because none of the measures in these other areas is perfect. Detection and recovery controls include:

- **Audit -** The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches.

- **Intrusion Detection and Containment -** It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner. It is also of little use to detect a security breach if no effective response can be initiated. The intrusion detection and containment control provides these two capabilities.

- **Proof of Wholeness -** The proof-of-wholeness control (e.g., system integrity tool) analyzes system integrity and irregularities and identifies exposures and potential threats. This control does not prevent violations of security policy but detects violations and helps determine the type of corrective action needed.

- **Restore Secure State -** This service enables a system to return to a state that is known to be secure, after a security breach occurs.

- **Virus Detection and Eradication -** Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity.

As a basis for planning, GoG should consider security services that support full compliance with security on privacy laws, regulations, and policies. These services include *identification*, *authentication*, *authorization*, *encryption, non-repudiation and Public/Private Key Infrastructure (PKI).* The key information security concepts that these services must address centers around the five key words – confidentiality, integrity, availability, auditability, and accountability - found at the vertices of the star in Figure 15 on the next page.

Figure 15: Key Information Security Concepts

Confidentiality: this is the concept that information is made unavailable (not disclosed or revealed) to those who are unauthorized to access it. People should only have access to data, which is necessary to perform their job function. The concept of allowing access to information or resources only to those who need it is called *access control*.

Integrity: this concept deals with the prevention of unauthorized creation, alteration, or destruction of information. Integrity ensures that information cannot be modified in unexpected ways, assuring *accuracy* of the information. Integrity protects against threats to the validity of data.

Loss of integrity could result from human error, intentional tampering, or even catastrophic events. Information may be *encrypted* (transformed into some secret form) to prevent unauthorized individuals from using the data.

Availability: availability prevents resources from being deleted or becoming inaccessible. Also, it ensures that legitimate users are not unduly denied access to information.

Auditability: this concept is concerned with network and database administrators and ICT auditors collecting data and analyzing it to verify that the users and

authorizations rules are producing the intended results as defined in an organisation's security policy.

Accountability: accountability deals with individual attempts to violate the security policy.

Developing the E-Government Security and Privacy Framework

Consistent with its approach to other major elements of the E-Government Framework, a phased approach to its security and privacy efforts needs to be adopted.

The required activities are:

- conducting risk assessment of GoG's major applications, general support systems, and financial systems, resulting in a better understanding of security risks and an improved ability to address them;
- developing system security plans for major applications, general support systems, and financial systems;
- developing an enhanced computer security awareness training plan;
- establishing an annual review cycle of audits;
- integrating ICT security into each phase of the E-Government's project life cycle;
- developing a comprehensive GoG policy for computer security;
- developing computer security guidance and publishing a GoG Information Security Guidelines Handbook, and
- initiating a program of assistance for MDAs to comply with the GoG Information Security Guidelines Handbook.

The E-GMS should consider using a best approach when implementing security on LANs, Voice over Wireless LANs (VoWLANs), WANs, and Virtual Private Networks (VPNs). The most proven and widely-accepted approach is the Five Layered Security Approach which is discussed next.

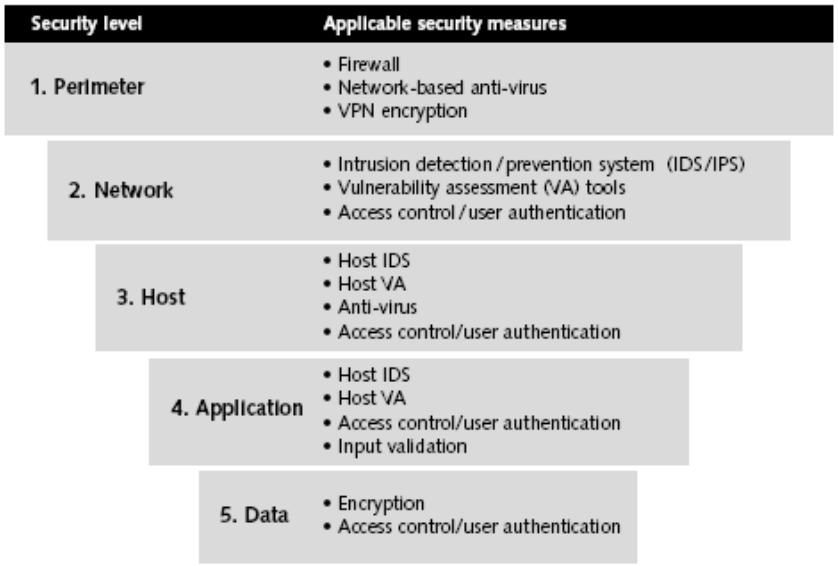
The Five-Layered Security Approach

This approach segments the organization's security into five (5) levels as depicted in Figure 16 on the next page. The five levels are the:

1. Perimeter
2. Network
3. Host
4. Application

5. Data

Figure 16: The 5 Security Layers



Source: StillSecure

The Perimeter Level: The network perimeter is the area where a LAN ends and the Internet begins. It is the first line of defense from outside un-trusted networks. The perimeter consists of one or more firewalls and a set of strictly controlled servers located in the Demilitarized Zone (DMZ). The DMZ contains the Web Servers, email gateways, network anti-virus (blocks infected email traffic by quarantining suspicious and infected email messages and then notifying recipients and administrators), and DNS servers that are exposed to the Internet. The techniques and tools used to provide security at the perimeter level are firewalls, network anti-viruses, and VPNs.

The Network Level: refers to security within LANs and WANs. The techniques used at this level are Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Vulnerability Assessment (VA) tools, and Access Control/Authentication systems.

The IDS and IPS analyse network traffic into greater details than firewalls. IDS tools alert staff that an attack has occurred. IPS products alert staff of the occurrence of an attack and block the harmful traffic. To be effective, an IPS must be placed in-line with firewalls, and on the side of the firewall exposed to the Internet (outside).

A network Vulnerability Assessment tool scans devices on a network for flaws and vulnerabilities that could be attacked by hackers or harmful traffic and outputs a list of discovered vulnerabilities, which can then be assigned to ICT staff for remediation.

The Host Level: Hosts are servers, desktops, switches, and routers, which have configurable parameters (registry, patches, services operated on the device, and so

on) that, when inappropriately set, create holes that can be exploited by malicious traffic.

Host-based IDSs monitor traffic on a single network device. Host-based VAs scan traffic on single network device. Device-specific network anti-virus can also be deployed on these hosts. However, they are very expensive to deploy and it takes a long time to get them fully operational. Access Control/Authentication systems must also be deployed at this level.

The Application Level: All applications ranging from custom-built ones to commercial off-the-shelf ones are all bug-ridden and full of exploitable vulnerabilities. In order to secure them from malicious attacks, it is usual to deploy application shields on web and database servers, and validate input (verify that application input traveling across the network is safe to process. Access Control/Authentication systems also need to be implemented at this level.

The Data Level: Securing data requires a blend of policy and encryption. Encrypting data where it resides and as it travels across the network is a recommended best practice because it acts as a last line of defence should all the other security measures fail. The widely-accepted mode of data encryption is the Public Key Infrastructure (PKI) discussed in the next section.

Data security is highly dependent on an organization-wide policy that governs:

- who has access to data
- what authorized users can do with it, and
- who has ultimate responsibility for its integrity and safekeeping. Access

Control/Authentication systems should also be implemented at this level. **Security and Privacy**

Successfully implementing E-Government requires a level of trust on the part of all transacting parties. Government MDAs, private businesses, and individual citizens must believe that electronic execution of private and/or sensitive transactions (such as providing regulatory data, bidding on a contract, or making a benefit claim) will be conducted in a way that ensures protection of information. E-Government security and privacy protection activities address the protection of the government assets involved in E-Government. These actions protect and defend information and information systems by ensuring confidentiality, availability, integrity, authentication, and non-repudiation.

This section addresses implementation of PKI and an assessment of the impact of privacy issues related to ICT systems.

Implementing Public Key Infrastructure

In establishing a trusted collaboration infrastructure, an overall electronic signature capability must be developed. A Public Key Infrastructure (PKI) is the standard for creating a trusted collaborative infrastructure. In many instances, this PKI implementation will replace existing methods of authentication, provide encryption capabilities, and provide a reliable method of electronic signature.

Some examples of intended use include desktop, remote access, and website authentication; file and e-mail encryption; and e-Signature of forms, files, and e-mail. The PKI implementation will support, and in some cases require the use of, smart cards as the storage medium for certificates. Certificates are issued to provide portability and improved security of subscriber's private keys. The PKI effort will meet MDAs' long-term needs for security and E-Government.

Examples of security standards that the Ghana Government could adopt are listed in **Appendix E** of this document.

A secure network is the result of an ongoing security process and not simply the installation of security technology. This means that even with a strong security strategy in place, ICT must also actively monitor and enforce compliance with that policy, and be aware of the vulnerabilities inherent in the strategy they have chosen. **Industry Standards and Emerging Technology.**

Success in implementing E-Government depends on the extent to which the CBA will support the efficient and effective deployment, acquisition, use, operation and maintenance of ICT to support business operations. For this reason, there is the need to recommend a set of technologies that will support both industry-proven standards and emerging technologies.

Together, these technologies are a foundation for growth, interoperability, integration and expansion.

Platform Standards

MDAs will have to make significant capital investments on the selection and implementation of platforms that will support the new technologies that may be required. Enabling technologies will provide a migration path to a standards-based technology framework. To ensure that the framework arrived at supports a disparate audience, we need to focus on the following criteria:

- cross platform portability/operating system independence,
- mature (not antiquated) and/or emerging technology,
- loose integration of heterogeneous systems,
- infrastructure independence,

- standards-based platform,
- non-proprietary extensibility,
- ease of development and integration, and
- application interoperability and programming language support.

This criteria could be matched against a short list of platforms and messaging services such as J2EE, .NET, Web Services, Email and the File Transfer Protocol (FTP).

The Industry Standards and Emerging Technology, and Platform Standards are supported with the **Technical Reference Model (TRM)**, which is a hierarchical foundation (platforms and operating systems, data management, and business logic) used to describe how technology will support the delivery of application capabilities. The TRM outlines the technology elements that collectively support the adoption and implementation of component-based architectures.

The list in **Appendix F** is intended as a starter set of Industry, Technology and Platform Standards based on their relevance to E-Government.

Information Architecture

An information architecture will provide the content and form of **MDA information** and will address such issues as **executive decision-making information, management information, operational (tactical) information** focusing on the inter-relationships between applications and data, and the regrouping and storage of data in order to provide easy and reliable access to MDA information.

The **Executive Decision-Making Support System** will dwell on

- Policy formulation and planning, policy briefs,
- Sector management and performance reports,
- Strategic management reports/plans, and
- Summary management plans.

Management Information System will focus on

- Analytical Reports,
- Monitoring and Operational Reports,
- Planning Indicators/Strategic Management Plans, and
- Management/Operational Planning.

The **Operational (Tactical) Information System** will focus on:

- Data Entry and Processing,

- Statistical Reports, and
- Monitoring and Operational Data.

Strategic Goal 3: Implement a Secure, Robust, and Interoperable E-Government Infrastructure

To facilitate the implementation of E-Government, it will be necessary to build a new infrastructure that can provide customers of the government multiple integrated services over robust, secure and reliable connections. The key components of these connections will be the:

- communication infrastructure,
- network infrastructure,
- server infrastructure,
- Internet/web-based infrastructure,
- security infrastructure,
- application infrastructure, and
- knowledge infrastructure.

The core activities required to implement these set of infrastructure have been outlined in the next few paragraphs:

The Communications Infrastructure

The E-GMS has to:

- leverage SAT-3, VoltaComs and other communications providers' infrastructure to provide fibre-optic based communication platform for MDAs,
- deploy wireline and wireless broadband, and voice over wireless local area networks systems,
- deploy standards-based routing and switching infrastructure,
- implement cellular and mobile telephony,
- deploy interactive television,
- deploy location infrastructure that addresses data and links location to a consistent, language-independent map of the world that can be used to spatially index content and services, refine knowledge about user demographics, and attach location to content thereby enabling services to be pushed to users based on their location.

The Network Infrastructure

- Plan, design and deploy secured Local Area Networks (LAN), Virtual Local Area Networks (VLANs which offer logical sub-grouping, as either clients or servers, of the endpoint devices in a network, independent of how the devices are physically networked together through switches, bridges or routers), and VoWLANs (which use the 802.1x industry standard) for all MDAs.

  Government will be expected to take advantage of and extensively deploy Voice over Wireless LANs (VoWLAN) in particular. VoWLANs, which converge voice and data, are rapidly proliferating in developed countries. VoWLANs when deployed will also offer true value of packetized voice and computer telephony integration (CTI).

  The benefits of deploying VoWLANs include:

  eliminating extensive and expensive cabling,

  - increasing productivity because information is readily accessible in offices, conference rooms, hallways, labs and anywhere that employees require it,
  - improving communications – employees always remain accessible via email, instant messaging, and voice, and
  - better decision-making - anytime, anywhere access to real-time MDA
  - information means employees are “in the know” all the time.

  Most VoWLANs are simple to deploy and they combine:

  - dynamic and intelligent radio frequency (RF) management (dynamically detecting and adapting to changes in the RF environment regardless of network load or network topology),
  - seamless mobility,
  - advanced Quality of Service (QoS), and
  - wireless protection into a single scalable, reliable, and cost-efficient platform. They are self- configuring (require minimal human intervention), self-healing, and support such encryption protocols as IPSec, Wireless Equivalency Protocol (WEP), and Wi-Fi Access Protocol (WAP).

  VoWLANs employ graphical tools to view network characteristics such as:

  - bandwidth utilization,
  - channel assignment,
  - noise level, and
  - signal strength.

  They also have features to detect alarms, detect rogue devices, and detect and prevent denial-of-service attacks.

- Bluetooth is a set of radio frequency (RF) communications protocols and standards that enable low-cost, high-speed communications among devices within 10 meters (this distance increases to 100 meters with amplifiers or higher transmission power) of each other that MDAs could consider deploying. The technology, provides wireless personal area network (WPAN) connectivity between consumer electronics and devices, replaces point-to-point wires for a variety of applications.

  Today, a conventional mobile phone hands-free kit uses a wire to connect the microphone and earpiece to the telephone. Similarly, a conventional PDA (or a digital camera) requires a cradle, cable, and a USB connector to synchronize with a PC. Bluetooth-enabled hands-free kits and devices will dispense with these wires and connectors. A notebook computer can then connect wirelessly to a LAN in an office, a modem in a mobile phone, or a desktop PC. A wireless headset can work with a mobile phone or automatically connect to an office or home telephone. Bluetooth can also be used to network household appliances to each other.

  Bluetooth technology, which transmits both voice and data, replaces both cable and infrared (IR) links. Although Bluetooth cannot match the speed of IR communication, it does not have IR's line-of-sight limitation and transmits both data and voice communication. Because line-of-sight is not necessary, a Bluetooth device can remain connected while moving. Bluetooth also has some capability to penetrate objects such as windows, cubicle dividers and even walls. Bluetooth devices can interoperate seamlessly with 802.1x networks.

- Plan, design and deploy a secured Wide Area government network and Internet connectivity for all MDAs

- BlackBerry, a belt-worn e-mail/organizer with two-way wireless communication capability can be linked to a PC for users to synchronise their calendars, telephone books, and to-do lists. When BlackBerry is removed from its cradle and carried around, it becomes an extension of the user's e-mail account, which the BlackBerry software monitors.

  When a message is received, the BlackBerry software encrypts a copy of it and sends it over the Internet to a gateway, and, from there, over a network, which delivers it to the BlackBerry handheld device. The handheld device decrypts the message and stores it.

  A user replies to the e-mail using a small keyboard, and the reply is encrypted and routed to the BlackBerry software on the desktop PC or a server. The BlackBerry software decrypts the message and sends the message from the e-mail account. Messages sent from the BlackBerry handheld, thus, are functionally equivalent to those sent from the desktop. Both originate from the same e-mail address, and copies of both are placed in the user's Sent Items folder.

  File attachments to incoming e-mail messages are not sent to the BlackBerry device. Instead they are held on the desktop computer. The user is notified that there is an attachment and informed of the type of file. If the user decides to forward the message to another e-mail address, the e-mail is sent from

BlackBerry back to the user's desktop, where it picks up the attachment and sends it along with the forwarded e-mail.

- Plan, design and deploy, for specific MDAs, Virtual Private Networks (VPN), which are private data networks that make use of public communication infrastructures and maintain confidentiality through the use of a tunneling protocol and associated security procedures. A VPN is the practical answer to the government's need for connectivity. Instead of using expensive, and sometimes unavailable, dedicated leased lines to implement Wide-Area Networks, GoG can deploy a VPN, which uses comparatively inexpensive shared infrastructure such as the Internet and the phone system. A VPN can support field office to central office connections, links between agencies, and even public access. Laptops can even be used in the field to access an MDA's Intranet and databases. The main advantage of the VPN approach is that it leverages technology and skills that many ICT managers already possess and is vendor neutral in terms of access points. This means that it is deployable almost immediately with very little learning curve.
- Set up a central government Network Administration Service.

The Server Infrastructure

- Implement an n-tiered server system (front-end web servers, middle-tier application servers, and back-end database servers),
- Deploy a flexible and robust directory system (e.g. X.500, Active Directory, Lightweight Directory Access Protocol).

The Internet/Web-based Infrastructure

- Deploy the universally accessible Internet infrastructure in all MDAs,
- Deploy intranet and extranet facilities in all MDAs,
- Set-up Government Official Portal and MDA Websites.

The Security Infrastructure

- Deploy trust infrastructure (built upon encryption techniques that use public and private keys to construct digital certificates to identify individuals and organizations),
- Deploy biometric-based security systems,
- Ensure the Deployment of Firewalls and Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS),
- Deploy Disaster Recovery Services,
- Deploy Emergency Response Services.

The Application Infrastructure

- Deploy Common Applications including
  - Set-up Help Desk Services
  - Set-up Electronic Mail & Messaging Services
- Deploy Special Applications including
    - Frontline Service Information Systems
    - Public Services Information Systems
    - National Crime Information Systems
    - Government Electronic Procurement Systems
    - Integrated Personnel and Payroll Systems
- For custom-built software, deploy programming infrastructure based on
    - Graphical User Interface (GUI) components
    - Utility (service) components (provide services needed to speed up application development, e.g. database access, messaging, etc.).

The Knowledge Infrastructure

There are two forms of knowledge infrastructure: the database-based infrastructure (for structured data) and the Enterprise Information Portal (EIP) based infrastructure (for unstructured and semi-structured data).

EIPs provide a one point access to knowledge and application resources through the familiar web browser interface, and are fast replacing intranets. As a minimum, EIPs must have the following capabilities:

- text search and retrieval,
- personalization and collaborative filtering,
- taxonomies and linguistic analysis for knowledge mapping,
- document management capabilities (or links to management systems) and workflow, and
- collaboration.

Both databases and EIPs use knowledge management technologies to capture, store, catalog, protect, retrieve, and disseminate information.

For the database infrastructure the Ghana Government has to:

- implement a highly-available, rapidly-scalable networked information storage system (storage systems that are linked by a network) which offers continuous access to data,
- deploy Data Warehousing and Data Mart Services for such systems as
    - Government Physical Assets Database System
    - Public Records, Management and Archives Database Systems
    - Statistical Database and Information System
- employ relational on-line analytical processing, data mining, query and reporting, and OLAP techniques.

For Enterprise Information Portal Infrastructure:

- establish a content delivery infrastructure for web-based systems,
- deploy Content Management Applications (for incompletely structured data),
- deploy Content Management Repositories,
- deploy web-based collaboration products and services,
- implement document management and workflow systems.

Strategic Goal 4: Ensure the Legal and Regulatory Framework supports the adoption and implementation of E-Government.

The Legal Framework for E-Government has to take into consideration:

- access to information and the protection of citizens' rights,
- privacy of personal information,
- protection of rights to software products and databases,
- specification of criminal liability stipulated for computer offences,
- reflection of all institutional, national and international requirements in existing strategic and statutory documents,
- development of an overall legal framework and standards for the use of ICT for public services,
- clarification of the responsibility for providing true and complete information, stored and processed electronically,
- regulating content such as hate speech and pornography,
- does a country have jurisdiction over Internet activities originating from other countries?

Strategic Goal 5: Leverage the use of ICT, within an effective E-Government Environment, to meet vital socio-economic development goals.

ICT could be used to meet vital socio-economic development goals such as:

- improving governance
- alleviating poverty
- providing basic health care
- enhancing education via distance and e-learning, interconnected schools, virtual libraries and virtual laboratories, and providing flexible education opportunities for rural students, out-of-school youth or unemployed rural residents
- improving agriculture
- fostering a dynamic business climate for entrepreneurs
- providing an enabling climate for small and medium sized enterprises, and assisting them to access financial and logistical support
- facilitating access and exchange of information between and among government, civil society, NGOs, the private sector, and ICT industries and
- enhancing the law and judicial processes.

To meet this strategic goal, the E-GMS should:

- **Undertake E-readiness assessment** in all districts and the local agencies of bi- and multi-lateral donors. The assessment should be conducted with such variables as connectivity, availability of ICT human capital, adequateness of information security, and potentials for E-Leadership. The results should provide the relevant information to assess the current status and help establish a baseline for E-Government policy, regulation, standards, and human resource requirements.
- **Assist in the integration of ICT applications in donors' activities** to improve the flow and use of information and knowledge for the effective execution of supported projects and activities. Some of such applications are:
  - Geographical Information Systems (GIS) to help protect land and natural resources
  - Telemedicine to support health care in rural areas, and
  - Distance learning to support education and skills building in remote areas.
- **Develop multimedia content on web pages and as video presentations** that would make the messages delivered to the rural folks more interesting, locally relevant, and developed to fit the needs of target audiences in local language and dialects, taking local culture into consideration.

- **Establish Multipurpose Community Telecenters (MCT) in collaboration with such donor agencies as (CIDA, UNDP, UNESCO, and ITU)** to bring ICT and access to information into the rural areas
- **Promote strategic alliances and partnerships** with existing ICT initiatives at national, regional, and international levels, and establish principles of effective public-private sector partnerships.
- **Advocate for, and possibly spearhead, the establishment of a Center for Learning, Information, Communication, and Knowledge (CLICK) for ECOWAS countries** to improve the dissemination and use of information and knowledge for development, as well as the use of best practices, through ICT.

Strategic Goal 6: Seek Active and Direct Participation of the Private Sector in the Implementation of E-Government

Government will never have sufficient manpower, both in terms of quantity and quality, to implement and operate all identified E-Government infrastructures. It therefore has to encourage the outsourcing of some of these infrastructures to the private sector to get them efficiently and effectively implemented. The objectives of the outsourcing of E-Government infrastructure are to allow government to:

- concentrate on its “core” business of governing,
- save ICT costs,
- implement a variable cost approach,
- obtain immediate cash infusion (typically associated with the transfer of assets to the vendor),
- improve overall performance,
- keep current with industry ICT trends,
- provide access to new technologies,
- reduce risks,
- share risks,
- implement tools for growth,
- standardise diverse systems,
- revamp the ICT structure management,
- facilitate migration to new systems,
- manage legacy systems,
- refresh existing systems,
- manage legacy systems while the customer implements new technology,
- obtain new or additional resources, and

- provide flexibility to increase/decrease resources.

As part of the outsourcing process, it will be worth the government's while to outline the benefits and risks of outsourcing and assess whether the benefits outweigh the risks.

Benefits of Outsourcing

Some of the benefits that will be derived from outsourcing the establishment of some of the identified infrastructure to the private sector include:

- cost savings/benefits
- enhance ability to concentrate on core business
- implementation of organisation-wide initiatives
- sale of assets (moving assets off books, capital infusion)
- greater resources to move to new environment/systems in a faster timeframe
- more/varied skills and resources
- better access to new technology
- reduced training expense, and
- enhanced flexibility.

Risks of Outsourcing

- loss of control
- cost management
- tax liability
- difficulties in re-assuming responsibility (or "insourcing"), and
- reduced flexibility

Private sector organizations can assist E-Government's implementation by:

- assisting MDAs to develop, review and finalise project terms of reference (ToR), technical and functional specifications, and requests for proposals (RFPs),
- developing and supplying common/specific application software for MDAs,
- undertaking Build Operate and Transfer (BOT), Build Operate and Own (BOO), and Build Transfer and Operate (BTO) arrangements for large revenue generation and other systems, where the returns on investment are clear or where there are obvious benefits in the implementation of the systems but the agencies are constrained by cash flow requirements of the project,

- supplying hardware and software through leasing or lease-to-own arrangements,
- supplying maintenance and technical support, training and change management services, and system integration services,
- creating an electronic database by converting paper-based data to digital form for major systems with large volumes of data,
- providing efficient and effective communication systems for data, image, voice, and related infrastructure; and
- supplying technical ICT personnel on short -term or long-term basis for agency-defined work and outputs.

The following minimum set of policies and actions need to be adopted to encourage private sector participation in E-Government implementation:

- formulate clear implementing rules and regulations on the BOT/BTO/BOO law for ICT projects,
- proper articulation of the policy of outsourcing of system development and other ICT services as an alternative to in- house development,
- develop performance-based service contracting procedures that clearly define the performance specification and deliverables for the acquisition of ICT products and services,
- provide incentives on intellectual property rights for systems that can be used by many agencies, and
- develop clear user and system specifications available to those offering services or products.

Section 6. E-Government Road Map

Strategic Direction

The model on the next page (Figure 17) shows how the foundation components of E-Government support the change processes through the following phases:

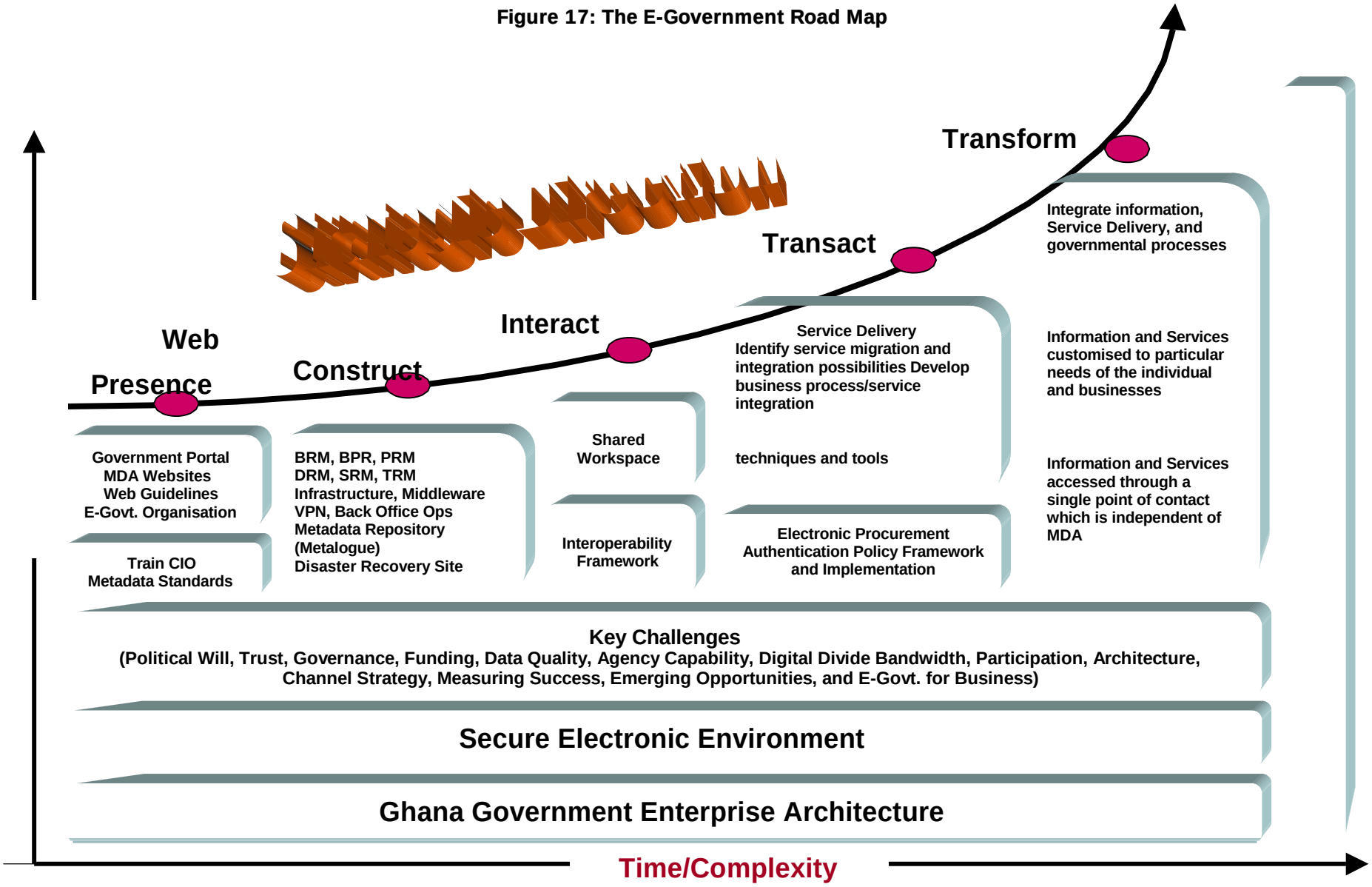
- Web presence
- Construction
- Interaction
- Transaction
- Transformation.

Each phase of the process is described below:

Phase 1 – Web presence

- MDAs provide a website to deliver basic information to the public. It is important to achieve, as soon as possible, a "critical mass" of government agencies connected to and using the Internet, which will serve as the means of communication and information dissemination in government.
- Establish a government portal, which will provide a single point of entry for accessing public government in order to facilitate public access to information. The portal must also have a search engine to allow users to quickly locate the sites that may contain the information needed.
- Government establishes E-Government Management Structure (E-MGO)
- E-MGO establishes web guidelines
- E-MGO establishes metadata standards
- MDAs deploy document management and workflow systems to improve handling and processing of document records
- Train Chief Information Officers.

Figure 17: The E-Government Road Map



Phase 2 – Construct

- E-Government Management Structure establishes reference models, infrastructure, middleware, a metadata repository, and a data warehouse of government information. Together with Executive Information System and Decision Support Systems, a government data warehouse will offer the capability of harnessing transactional data from multiple sources.
- Government deploys a distributed database model. The devolution of functions and the nationwide operation of government make distributed database technology ideal for integrated government applications. Harnessed properly, it provides the solution for the proliferation of stand-alone applications in government, and allows existing systems, particularly hardware, to be retained with some modifications. The ability of distributed databases to allow data to be physically kept locally while providing logical integration is ideal for central and field offices set up in most organisations, allowing data to be accessed wherever it is located. The support for local data entry, processing, and storage of information will also alleviate delays in transmitting data from the field. Distributed databases will facilitate sharing of information across MDAs, thereby reducing the need for duplication of data and applications.
- Establish a VPN as the nationwide WAN of government. This could be achieved by simply installing VPN access routers in all Internet-connected sites, defining and implementing an encryption strategy, and upgrading leased line connections of agencies to Digital Subscriber Lines (DSL) to meet the concomitant data traffic.
- Adopt a web-based model for government applications and services. This will provide a standard easy-to-use, graphical user interface that is identical for both local and remote users. Existing database servers may be made to support more users through dedicated Web servers. This model will inherently support scalability of systems in that processing load can be readily and transparently distributed across multiple servers. Once implemented, servers and clients may be upgraded or replaced independently of each other, thereby allowing system replacement costs to be spread out over several years.
- Connecting government systems to the Internet will expose them to hackers, unauthorized users, viruses, and other risks. To address this, a security infrastructure, which will be a combination of technology, policies, legislated laws, and enforcement procedures, has to be deployed.
- The use of tested security technologies and best security practices in implementing E-Government has to be an overriding priority of the plan. Security beyond the standard firewalls has to be adopted and deployed to protect systems with valuable data. The public web server must remain "outside" the agency's firewall. Secure encryption techniques

must be employed on all VPN links. Systems must be designed to reject "crackable" passwords, and strictly implement password aging. For E-Commerce applications and government business transactions, authentication devices like smart cards, client membership procedures like membership enlistment, and enforcement mechanisms like user Certification Authority must be strictly implemented in combination with standard identification systems and procedures.

- The government will embark on catalyzing the creation of an “intelligent nation” by embarking on a scheme that subsidises the purchase of hardware and software by all public servants on flexible credit terms.

Phase 3 – Interact

MDAs extend the capability of their website so people who used to visit a government office now:

- have online access to critical information
- can contact the office by email
- can download forms from the Internet (one-way interaction), and
- can complete and submit forms on the Internet, including identification of the person (two-way interaction).

Government must, as a matter of urgency, collaborate with the Ghana Post Company to install “community point” information kiosks or Personal Information Terminals (PIT) throughout the post offices in the country. These kiosks should be equipped with computers, which ideally should have a touch screen, a traditional keyboard, and a printer (which could later on be upgraded with a smart card reader, a video camera, and a microphone), and hooked to the internet, will be designed to:

- provide swift access to government information and services
- provide self-help information, and ultimately,
- introduce online shopping to local communities.

Phase 3 – Transact

- MDAs add self-service applications to their websites so that people can complete entire transactions (execute events, decisions, and payments) or processes online.
- The web begins to complement other service delivery channels, providing around the clock access independent of users’ geographic location.
- Increasingly, MDAs develop services that involve different MDA business delivery systems that are seamlessly integrated.

Phase 4 – Transform

- The delivery of government services and potentially the operation of government itself are redefined,
- Information, service delivery, and governmental processes are integrated across traditional boundary lines,
- Information and services are increasingly customised to the particular needs of individuals and businesses,
- The identity of individual MDAs matters less to people as information and services are accessed through a single point of contact on the web,
- E-Government reshapes the relationships between government, individuals, and business.

The key E-Government implementation stakeholders are the:

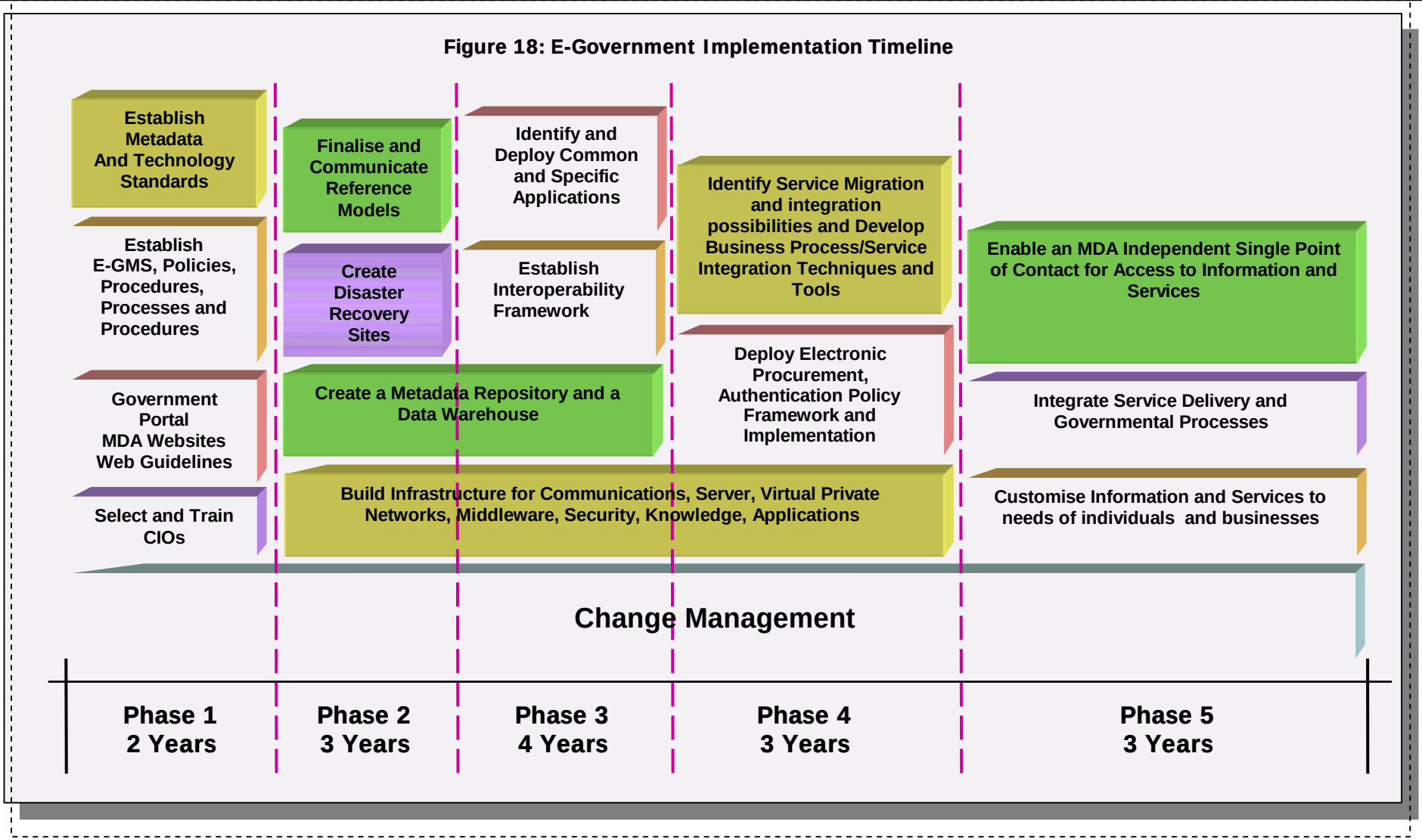
- Ghanaian citizenry,
- Sector Ministries and their Departments and Agencies,
- Regional Coordinating Councils,
- Municipal/Metropolitan and District Assemblies (MMDAs),
- Public Services Commission,
- State Enterprise Commission,
- Trade and Labour Unions and Associations, and
- Business Community.

Programme Prioritisation and Implementation Timelines

Figure 18 on the next page indicates proposed prioritization of E-Government programmes and implementation guidelines and timelines. Since many countries have started implementing E-Government, it is expected that Ghana will not re-invent the wheel by starting from scratch, but will avail itself of the myriads of relevant information that abound on the World Wide Web. This will enable Ghana hasten its implementation by adopting an aggressive mode thereby halving the long timelines experienced by the E-Government pioneers.

Broadly, government is expected to establish an E-Government Management Structure, which will in turn establish E-Government policies, procedures, processes, and practices within the first two years of its operation. By this time, it would be expected that each MDA would have established a web presence.

Figure 18: E-Government Implementation Timeline



Within the same two-year period, the E-GMS will establish metadata and technology standards, web guidelines, and select and train CIOs.

Next, the E-GMS will be expected to finalise and communicate the reference models of the Ghana Government Enterprise Architecture to stakeholders and create disaster recovery sites, start the creation of a metadata repository and a data warehouse. By the end of phase 3, it would be expected that the E-GMS has established an interoperability framework, and identified and deployed common and specific MDA applications.

Having established the necessary framework and standards, the EGMO would be expected to have a governmental VPN, and put in place other infrastructure (for communications, networks, applications, server, security, and applications) by the end of the fourth phase. During this period, the E-GMS would be expected to undertake the identification of service migration and integration possibilities and develop business processes/service integration techniques and tools

In phase 5, the E-GMS would be expected to integrate service delivery, deploy electronic procurement, and enable an MDA-independent single point of contact for access to information services.

Regional Integration (NEPAD)

Because of governmental and socio-economic interactions between Ghana and its neighbouring countries, Ghana's E-Government initiatives cannot be implemented in isolation. There has to be homogeneity in pursuing and establishing E-Government standards, guidelines and systems in the sub-region to enable government-to-government interaction and collaboration in:

- providing the necessary impetus to the democratization process and good governance,
- facilitating the integration of Africa into the new knowledge society,
- providing training to create the much needed critical mass of ICT professionals in the sub-region,
- leveraging technology to exchange research knowledge to meet Africa's specific needs (of fighting illiteracy and alleviating poverty and hunger),
- managing conflicts,
- establishing regional distance learning,
- controlling of pandemic diseases and instituting effective health education programs, and
- exploiting opportunities for trade.

To achieve this, Ghana has to strengthen its cooperation in the E-Government arena and between itself and other countries in Africa. Implementing E-Government in the

sub-region will accelerate Africa's integration into the global economy. Ghana therefore has to collaborate with other African countries by:

- promoting discussion of e-government topics by setting up a working-group on E-Government formed from public and private sector bodies in the countries concerned, and
- arranging study visits to each country to help identify areas of cooperation for planning E-Government initiatives.

Ghana needs to identify itself with the "e-Africa initiative" launched by CAFRAD in 2002. This initiative aims to raise awareness on the role that ICT can play in the development process. The "e-Africa initiative" focuses on drawing on the strengths of both good governance and ICT and wishes to provide an important contribution to the success of NEPAD's overall vision for Africa's development.

E-Government Roles

For the implementation of E-Government to succeed, the roles that major stakeholders (public officials, E-Government Management Structure, and MDAs) have to play have been outlined in the next paragraphs.

Public Officials

All public officials need to appreciate and use basic technology (especially the Internet) – ICT is critical to delivering E-Government outcomes.

E-Government Management Structure

The role of the E-Government Management Structure has been discussed in Section 5.

Ministries, Departments and Agencies

All MDAs have roles to play – involvement should be made mandatory. Cabinet approves the core aspects of E-Government and gives directives to MDAs. All MDAs should:

Plan

- Incorporate E-Government into their objectives, strategies, and business plans from January 2005 onwards.

Prepare

- Make delivering E-Government a high-ranking management responsibility,
- Institutionalise E-Government by creating or assigning functional responsibility to a particular organisational unit,
- Spread accountability for delivering E-Government through all levels of the organization,
- Start recruiting and retaining people with the skills to deliver E-Government,
- Develop the capability to understand people's (citizen's) wants, needs and abilities to interact with the MDAs online,
- Prepare the organisations to operate in an integrated environment,
- Eliminate or change activities and projects that are not aligned with E-Government initiatives.

Participate

- Participate in E-Government networks, seminars, workshops, and conferences,
- Actively seek opportunities to deliver E-Government in collaboration with other MDAs,
- Educate customers and stakeholders on how they can benefit from E-Government,
- Strive to meet mandatory requirements such as authoring metadata and complying with the interoperability framework,
- Ask to be included in E-Government projects and activities that are congruent with the department's activities,
- Integrate the common foundations of E-Government into the organisation's business environment.

Section 7. E-Government Challenges and Limitations

As expected with such an effort as pervasive as that concerned with the implementation of E-Government in Ghana, there will be some challenges. Furthermore, E-Government ought not to be perceived as a panacea to all public administration and governance problems. This section therefore concerns itself with anticipated challenges and limitations of the E-Government initiatives.

E-Government Challenges

The identified E-Government challenges are:

- **Implementing E-Government requires a coherent strategy**. It requires:
  - political will
  - adequate planning
  - sustained dedication of resources
  - total commitment by all stakeholders, and
  - an appropriate legal and regulatory environment.
- **Citizens need to trust government** - Citizens will require confidence that their personal privacy is not threatened. This requires on-going efforts in developing the right ethics, values and standards within government organisations. A robust privacy environment (legal and regulatory framework) that checks against misuse of personal information has to be created.
- **Government has to find ways of trusting citizens** - There has to be a policy framework for online authentication.
- There is also the need to **build trust** within MDAs, between MDAs, across governments, with businesses, non-governmental organizations, and citizens.
- **E-Government will present a new way of (and consequently, a new challenge for) doing business for government -** As MDAs become more interconnected, there will be challenges for public sector and civil service governance. In particular, there will be the need for new decision-making processes that support integrated back office and service delivery strategies and business process.
- **Inadequate bandwidth and accessibility -** The lack of nationwide broadband connectivity and its attendant problem of rural people not being able to access information on the Internet is a major challenge.
- Monopolies charge **exorbitant prices** for the use of bandwidth.
- **Low tele-density -** The current tele-density of 4% (as at March 2004) is too low for the wide participation needed for E-Government to be successful.

- **Poor quality of data and information management practices** - E-Government will present new ways for clients to interact with government electronically. These imply the ability to seamlessly and securely exchange or share data between business systems, both within and across MDAs. Implementing E-Government initiatives means MDAs ought to brace themselves to confront issues of data with variable quality and variable consistency.
- **Interoperability** - Currently, information is being stored, accessed and managed differently on disparate software and hardware platforms across MDAs. Creating an E-Government Interoperability Framework will resolve most of these problems.
- **The digital divide -** The full benefits of E-Government will be realised when as many Ghanaians as possible have access to the Internet, and the attitudes and skills to make effective use of it. E-Government may exacerbate inequities among citizens (especially the marginalised or underserved – women, illiterate citizens, senior citizens, and the poor.)
- **Participation -** Participation in the online world poses a number of challenges, ranging from ensuring equity of opportunity through to establishing that people are who they say they are, and, therefore, that their contributions are valid. Online services must be designed to serve all members of society irrespective of their physical capabilities.
- **E-Government for business -** The E-Government Management Structure (E-GMS) has to work with business-focused MDAs to ensure the MDAs buy into E-Government initiatives, and that the initiatives are coordinated to deliver the maximum benefits for the business community.
- **Funding -** Finding out how much funding will be required for E-Government activities, and how this requirement will be met will be a major challenge.
- **Identifying and seizing emerging opportunities** and responding to them appropriately.
- **Building capability in MDAs -** E-Government demands that all MDAs, supported by the E-Government Management Structure, develop new and diverse capabilities. For example, MDAs will have to:
    - learn how to make the best use of the Internet to reach their citizens
    - integrate E-Government into their overall strategic planning
    - adapt themselves to an environment in which more information and technology is shared or subjected to all-of-government (a-o-g) policies and standards, and
    - find ways of collaborating with other MDAs in potentially complex webs of integrated service delivery.
- **Building capacity in the citizenry -** Citizens will have to learn how to reach government on the Internet.

- **Building capacity (technical, managerial, and political) in the Chief Information Officers** who will be champions during the implementation of E-Government.
- **Public education -** Public awareness creation, sensitisation and communication of E-government benefits need to be well effected.
- **Measuring the uptake and effectiveness of E-Government -** On a regular basis, the E-Government Management Structure has to find ways of measuring:
    - how much progress MDAs have made in creating and delivering E- Government, and
    - how useful E-Government is to the citizenry and businesses.
- **Resistance from staff of the MDAs because they fear that:**
    - the new, automated processes will mean fewer opportunities to receive unofficial payments or bribes for services rendered,
    - their authority will be diminished with the introduction of E-Government, and
    - they have nothing to gain professionally from adapting to new technology.
- **Using e-mails as a means of communication** challenges formal notions of how government correspondence should be dealt with (communicating certain matters by e-mail is inappropriate - for example, using e-mail to dismiss an employee would be considered insensitive).
- **Intranets and the sharing of information** in organisations can challenge the traditional flow of information in a hierarchical organisation.
- **Ensuring that laws are updated to recognise electronic documents and transactions** by taking proactive steps to ensure that policies support rather than impede E-Government.
- **New rules** may be required to govern the relationship or partnership between the public and private sectors.
- **Getting rid of regulatory frameworks, policies and arrangements** of government institutions that may deny Ghanaians the opportunities offered by the digital revolution.
- **Protecting E-Government sites from attack** from viruses, denial-of-service, etc., and misuse requires resources, including expertise and finance.
- Ways need to be found to bring **Wireless Fidelity (Wi-Fi) applications** to Ghana so as to make use of unlicensed radio spectrum to deliver cheap and fast Internet access.
- **Ensuring MDAs do not use ICT to automate existing processes -** They have to create more efficient and effective solutions that are now possible because of lessons businesses and governments in other countries have learnt from E-Business.

- **Stopping MDAs from buying systems that only address internal needs.** Such systems become disparate (islands of automation) and rarely able to interoperate or communicate with those in other MDAs. Consequently, these MDAs have not been able to easily share information, and citizens seeking information have had to search across multiple MDAs before finding the information. Businesses also have had to file the same or similar information multiple times at different agencies. For example, the same basic information about a particular firm may have been filed at Internal Revenue Services (IRS) and Social Security and National Insurance Trust (SSNIT) offices.

E-Government Limitations

E-Government will not

- solve all problems of corruption and inefficiency (technology savvy officials can find new opportunities for corruption),
- overcome all barriers to civic engagement,
- be a quick nor simple process (because it requires participation of the citizenry which is made up of people with different attitudes and skills),
- happen just because MDAs buy more computers and put up website,
- render automatic cost savings even though online service delivery could be more efficient and less costly than other channels.

Section 8. Managing the Implementation of the E-Government Strategy

As with all interventionist programmes, the E-Government effort needs to be managed in accordance with a proven programme and project management methodology. This section describes the key factors necessary for successful management of the programme, the documents required for the programmes implementation, and factors considered critical to the programmes successful implementation.

Programme Management

The key factors for efficient management of the implementation of E-government Strategy are as follows:

- **Political and governmental support at the highest level.** Commitment and responsibility of senior officials in the executive power at all stages of the process from the definition of the vision to the implementation of specific projects. Senior officials in the executive power take part in the management of e-government implementation process through all of its phases and assume responsibility for decisions made.

- **Active participation of citizens and business.** The participation of citizens and business in the management of the implementation process is a reliable tool for feedback and prevention of potential conflicts.

- **Teamwork and project-based principle of operational management.** The day-to-day operations management is performed on the basis of project management principles by interdisciplinary teams. The E-Government implementation calls for the involvement of formidable expertise potential in the field of information, communication and management technologies, as well as excellent knowledge of processes in the public administration.

- **Continuous coordination and feedback at all stages of implementation.** The effects of E-Government can be seen on a long-term basis, while its implementation requires enormous human and financial resources. The use of effective tools for current evaluation and proper impact will reduce the risk of waste of time and resources.

- **Strong methodological support.** The methodological support will ensure the compatibility of various information and communication systems, as well as transparency and efficiency of government, and save financial resources. This support is provided at the strategic level by methodological working groups, while at the operational level it is provided by methodological teams at the individual institutions.

- **Risk analysis and impact of risk factors (see below).** For any E-Government project to succeed, a comprehensive risk analysis must be performed. During the Initiation Phase, risks have to be identified at a high level. Risk analysis will enable the project team to proactively identify and prevent problems before they occur or by reducing the impact of problems when they do occur. Risks need to be continuously assessed throughout the project as the nature, probability, and impact of risks change by phase and activity.
- **Implementation of change planning and management.** A good appreciation of the risk factors will influence change management and planning. This should ensure that there is a process in place for effectively communicating programme goals and objectives, milestones, impact assessment, and expected changes. This must be done regularly, pitched at the right level to the stakeholders and the group of persons the programme will affect.
- **Providing for transparency in the public administration operations.**

Implementation Risks and their Mitigation

The impact of key decisions on the ultimate success of the E-Government implementation will need to carefully consider risk factors on an ongoing basis. These risks could be associated with any of the major components involved with the programme as detailed below:

People: Availability, (of suitably qualified people) their understanding and appreciation of each project/programme, perception of programme's management on their work schedules and quality of work.

Processes: Magnitude of change to existing business processes, security considerations, practical considerations and changes that can stand the test of time.

Technology: The choice of the appropriate technology, the need for the adoption of specific standards. The monitoring of selected standards to ensure a balance between opportunity and cost.

Effective management of risks involves:

- identifying possible risks in advance,
- having processes in place to monitor risks,
- having the right balance of control in place to mitigate the adverse consequences of the risk, should it materialize; and
- establishing a decision-making process supported by a framework of risk analysis and evaluation.

Active risk management helps the achievement of wider programme aims, such as:

- effective change management,
- the efficient use of resources,
- better programme/project management,
- minimizing waste and fraud,
- supporting innovation, and
- increased understanding and visibility of E-Government initiatives, leading to a more realistic estimate of timescale and costs.

An initial set of risks for E-Government implementation has been listed in the table below:

	Risk	Mitigation
1	MDAs too slow to adopt the E-Government strategy and migrate services on-line.	E-Government Management Structure supports MDAs and monitors their progress and report to Office of the President.
2	Government fails to capitalise on 'e' opportunities, especially integration opportunities that achieve economies and improved effectiveness.	E-Government Management Structure collaborates with MDAs to identify and pursue these opportunities, developing frameworks, models and tools to achieve economies and improved effectiveness
3	MDAs act independently of The E-Government Management Structure and make decisions inconsistent with the E-Government strategy.	All MDAs have to consult E-Government Management Structure on all e-initiatives.
4	Government does not make the most of MDAs initiatives that present opportunities across government.	Encourage MDAs to identify these opportunities early on and make the most of them.
5	E-Government Management Structure can't make the most of these opportunities (or minimise the risks) without the core work programme suffering.	Develop E-Government Management Structure's capability to work with MDAs around these opportunities

Change Management

Considering the magnitude and diversity of change required to make the E-Government implementation a success, it will be necessary to embark on a massive change management programme which entails:

- clearly and powerfully defining a comprehensive change vision and making it operational,
- building a quantifiable and sustainable business case for E-Government,
- assessing the change readiness of the MDAs, businesses and citizens and selecting the best change configuration,
- building the necessary level of stakeholder commitment through incessant communication and public education,
- defining leadership roles and responsibilities, and building leadership skills,
- developing the right culture with the appropriate mindset, values, and behaviour, and
- designing the right organizational structures at all levels (national, regional, district, and town) with appropriate reporting structures and integrating mechanisms, people performance management, and people practices.

Critical Success Factors

The following are the factors considered critical for the successful implementation of E-Government:

- strong visionary leadership,
- political will and commitment,
- provision of necessary logistical and financial resources,
- effective change management strategy,
- strong programme/project management,
- strong programme/project coordination,
- appropriate legal and regulatory framework,
- awareness and appreciation in the society of the need for E-Government development,
- education and training, practical skills of the human resource pool of users for participation in the E-Government,
- highly qualified ICT professionals,
- effective feedback.

Programme Management Documentation

A list of some of the documentation needed to manage the implementation of E- Government has been provided in Appendix J.

Practical Considerations for E-Government Implementation in the MDAs have been provided in Appendix I.

Appendices

Appendix A – Terms of Reference

The National ICT Policy and Plan Development Committee

TOR of the E-Government Technical Sub-Committees of the National ICT Policy and Plan Development Committee

1.0 The task for the Technical Sub-Committees

1.1 Each technical Sub-committee will have a team leader assigned to it by the National ICT Policy Plan and Development Committee.

1.2 A resource person will be recruited for each Technical Sub-committee and will be responsible for preparing the various draft documents for the consideration of the Technical Sub-committee. The resource person will be paid by the National ICT Policy and Plan Development Committee.

1.3 Each technical sub-committee will be responsible for reviewing the work of their Resource person and ensuring that the task carried out meet the required standard and the requirements of TOR given to the resource person.

1.4 The final draft of the output of each of the Technical Sub-committee will be submitted to the National ICT policy and plan development committee by the team leader for technical vetting and decision on the standard and quality of the work.

1.5 The national ICT policy plan development committee will have the final authority on deciding on the quality of standard of the final document submitted to it and on whether the submitted document meets the provisions of the TOR given the Technical Sub-committee and its Resource Person.

1.6 It is envisaged that the National ICT Policy Development committee will organize a stakeholder meeting on the draft outputs of each of the Technical Sub-committees to seek views that could lead to improving and finalizing the document by the relevant sub-committee

2.0 Details of the TOR for the Technical Sub-committees and the Resource Persons

2.1 Each of the technical sub-committee is tasked to develop a strategy and relevant programmes for implementing the relevant provisions of the Ghana ICT for accelerated Development [ICT4AD] Policy

2.2 Each strategy should take as its part of departure the relevant policy statements, provisions and measures documented in the ICT4AD Policy document. (In other words as part of making the case for developing the strategy the document should make extensive reference to; the relevant policy statements, policy commitments and policy measures of the government as contained in the policy document)

2.3 The strategy so developed should in broad terms answer the question:

'How the policy provision referred to will be implemented through specific mechanisms, measures, programmes and activities as per the Strategy'

2.4 Each of the strategy document being produced by each of the Technical sub-committee should also as a rule provide some indications of specific programmes, projects and initiatives that need to be put in place to implement the provisions of the strategy so developed.

3.0 Broad guidelines for the content of the strategy document of each of the technical sub-committee.

Each of the strategy documents should have the following sections:

3.1 Background statement

3.2 A review of the relevant focus area of the strategy, making references to the challenges, developments, and specific local and global issues pertaining to the subject area of focus of the strategy being developed

3.3 Make a case for the need for the strategy

3.4 Reference to the policy provisions for which the strategy is being formulated

3.5 Documentation and comment on the policy provisions and relating them to the subject area of the strategy

3.6 Documentation of the strategy section-by-section with each section tied into the relevant policy statements, commitments, and measures detailed in the policy document.

3.7 Documenting the programmes, initiatives and activities identified for the implementing the provisions and details of the strategy proposed.

3.8 Provide an indication for time-lines and prioritization of the programmes initiatives and activities identified for the Implementation the Strategy.

3.9 It is anticipated that each report will be less then 100 pages. But there may be cases where this number could be exceeded if the need be.

Appendix B – The 14 ICT4AD Priority Areas

1. Accelerated Human Resource Development
2. Promoting ICTs in Education – The Deployment and Exploitation of ICTs in Education
3. Facilitating Government Administration and Service Delivery – Promoting Electronic Government and Governance
4. Facilitating the Development of the Private Sector
5. Developing an Export-Oriented ICT Products and Services Industry
6. Modernization of Agriculture and the Development of an Agro-Business Industry
7. Developing a Globally Competitive Value-Added Services Sector - A Regional Business Service and ICT Hub
8. Deployment and Spread of ICTs in the Community
9. Promotion of National Health
10. Rapid ICT and Enabling Physical Infrastructure Development
11. Legal, Regulatory, and Institutional Framework Provisions
12. Research and Development, Scientific and Industrial Research Capacity Development
13. Promoting Foreign and Local Direct Investment Drive in ICTs, and
14. Facilitating National Security and Law and Order.

Appendix C - Check list on the compliance of E-Government Strategy document with ICT Policy

Policy Objectives and Strategies 3.3.3 (Promoting Electronic Government and Governance	E-Government Strategy Draft
To reform the Civil and public services to improve on their organizational systems, structures, procedures and processes	Provision has been made in section 4 pg. 7 of the draft document to address this issue through the proposed establishment of the E-Government Authority. Public Administration Services pages 8 & 9 and in pg 30&31 making the EA work
To address the poor attitudes to work and unproductive and inefficient work ethics which could hinder the effective exploitation of ICTs to improve organizational efficiency service delivery, productivity and reduction in operational cost within the civil service.	Provision has been made in section 5 of the draft document for ***Training and retraining of personnel in the public sector and civil service administration*** as part of the goals for the E-Government Strategy (pg.16)
To improve efficiency of the civil and public services and ensure that they play a more positive role in economic and social development at all levels	Provision has been made in section 5 of the draft document for ***Organizational and technological upgrading of the public sector and civil service administration*** as part of the goals for the E-Government Strategy (pg15)
To facilitate the establishment of an efficient intra-and-inter-departmental, inter-sectoral, national system of communication, for the necessary feedback in policy formulation and programme implementation, monitoring and review.	Provision has been made in section 5 of the draft document for ***Orientation towards citizens and businesses*** as part of the goals for the E-Government Strategy (pg. 15)
To modernize the operations of the Civil and Public Services through the deployment of ICTs to facilitate administrative cost reduction and their effectiveness and efficiency in the delivery of their services to the public.	Provision has been made in section 5 of the draft document for ***Organizational and technological upgrading of the public sector and civil service administration and Orientation towards citizens and businesses as*** part of the goals for the E-Government Strategy (pg.15)
To facilitate the development and implementation of a comprehensive e-government and governance strategy for Ghana.	The development of the E-Government Strategy document addresses the and specifically section 8 of the document is in managing and implementing the strategy

Appendix D – Metadata

Metadata is defined as “data about data”. It is a central point of reference for designing, constructing, retrieving, and controlling the warehouse data. E-Government metadata is critical to both technical and business users because it will provide guidance through any data warehouse or data marts that will be created for E-Government.

Technical Metadata identifies the following:

- **Where the data comes from** – internal or external data sources, system of record.
- **How the data was changed** – data mapping, consolidation procedures, transformation rules, and aggregation policies.
- **How the data is organized** – logical structure and content of the data warehouse.
- **How the data is stored** – physical structure and content of the data warehouse.
- **How the data is mapped** – to a multidimensional database format from a relational database format.
- **Data ownership/stewardship** – Who owns the data? Who is responsible for the data? What is the contact information?
- **Security** – Who can access the data?
- **System information** - date of last update, extract history, archiving criteria, and data usage statistics.
- **Scheduling information** - delivery schedules, scheduling details for data extracts, data transformations, and data loading.

Business metadata describes the following:

- **What data is available** – catalog of available data.
- **Where the data is** – location, access instructions.
- **What the data means** – description of the data contents, units of measure, definitions and aliases for the data, details of how the data was derived or calculated.
- **How to access the data** – business model of the data, indexes, keys.
- **Predefined reports and queries** – for getting the data.
- **How current the data is** – when the data was last refreshed.

Appendix E – Security Standards

01 X. 509 - International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Certificate Authentication

The international standard for the digital certificate authentication that is used for user identification, especially for creation of an electronic document used to prove identity and public key ownership over a communications network.

02 FIPS 186 - Digital Signature Standard (DSS) also Draft ANSI X9.30-199x Part 1; and ISO/IEC JTC1/SC27/M2, Project 1.27.08 Digital Signature with Appendix)

The DSS standard specifies a digital signature algorithm (DSA) appropriate for applications requiring a digital, rather than written, signature. The DSA authenticates the integrity of the signed data and the identity of the signatory. The DSA may also be used to prove that data was actually signed by the generator of the signature.

03 S/MIME - Secure Multipurpose Internet Mail Extensions

Provides a consistent way to send and receive secure MIME data. Based on the Internet MIME standard, S/MIME provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and data confidentiality (using encryption). S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP.

Reference: http://www.ietf.org/htmll.charters/smime-charter.html

04 SSL (Secure Sockets Layer)

An open, non-proprietary protocol for securing data communications across computer networks. SSL is sandwiched between the application protocol (such as HTTP, Telnet, FTP, and NNTP) and the connection protocol (such as TCP/IP, UDP). SSL provides server authentication, message integrity, data encryption, and optional client authentication for TCP/IP connections.

05 TLS (Transport Layer Security)

Standard for the next generation of SSL. Provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Reference: http://www.ietf.org/html.charters/tls-charter.htrnl

06 WS-Security (Web Services Security)

Describes enhancements to SOAP messaging to provide message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies including X.509, Kerberos, and SAML.

Reference:http://www.oasis-open.org/committees/wss/
http://www-106.ibm.com/developerworks/library/ws-secure***/***

07 SAML (Security Assertion Markup Language)

An XML-based framework for exchanging security information expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. SAMI, is expected to play a key role in the Federal-wide E-Authentication initiative, and is supported by both the Liberty Alliance and WS-Security.

Reference: http://www.oasis-open.org/committees/security/
http://xml.coverpages.org/saml.html

08 P3P1.0 (Platform for Privacy Preferences)

The Platform for Privacy Preferences Project (P3P) provides a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences.

Reference: http://www.w3.org/P3P/

Appendix F – Industry Standards and Emerging Technologies

01 Hypertext Markup Language (HTML)

HTML is a platform independent language used to publish information on the Internet.

Reference: http://www.w3.org/MarkUp/

02 DHTML (Dynamic Hypertext Markup Language)

A collective term for a combination of new Hypertext Markup Language (HTML) tags and options, style sheets, and programming that will allow Web pages that are more animated and more responsive to user interaction than previous versions of HTML

03 eXtensible Markup Language (XML)

XML is a platform independent, universal language used to support the structuring and integration of documents and data on the web. XML is a flexible set of standards for tagging/ classifying information so that it can be easily read and interpreted by people and data exchange systems.

Reference: http://www.w3.org/xml

XML offers the promise of simplifying the process in which organizations identify, integrate and process information that may be dispersed across incompatible systems and MDAs.

04 XHTML (eXtensible Hypertext Markup Language)

The W3Cs recommendation for the next generation of HTML leveraging XML

Reference: (taken from the FAWG E-Gov Guidance)
http://www.w3.org/TR/2001/REC-xhtml11-20010531/

05 XML Web Services

XML Web Services provide a simple, flexible, standard-based model for binding applications and business services over the Internet. XML Web Services are software components that can interact with one another dynamically via standard Internet technologies (i.e., HTML, SMTP, TCP/IP), making it possible for MDAs to communicate, share data and build bridges between disparate ICT systems that otherwise would require extensive development and integration efforts (i.e., middleware). XML Web Services are self-contained, self-describing, modular components/ applications that can be published, located, and invoked across the web regardless of hardware and software platforms.

Reference: http://www.w3.org/2002/ws/

06 Universal Description, Discovery and Integration (UDDI)

UDDI is the "yellow pages" of XML Web Services. UDDI is a platform - independent, open framework for describing and integrating business services over the Internet.

Reference: http://www.uddi.org

07 Simple Object Access Protocol (SOAP)

SOAP is an XML-based messaging technology standardized by the World Wide Web Consortium (W3C), which specified the necessary rules for locating XML Web Services, integrating them into applications, and communicating between them.

Reference: http://www.w3.org/TR/soap12-part1/

08 Web Services Description Language (WSDL)

WSDL is an XML document that describes a set of SOAP messages and how they are exchanged. WS131 uses an XML structure to describe message formats based on XML Schema.

Reference: http://www.w3.org/TR/wsdl

09 Microsoft .NET

The Microsoft NET platform includes a comprehensive family of products that power smart devices, services, servers, and tools designed to support XML and incorporate Internet industry standards. The .NET platform enables software integration through the use of XML Web services.

Reference: http://www.microsoft.com/net/defined/default.asp

10 Java 2 Enterprise Edition (J2EE) and Associated Specifications

The J2EE standard includes specifications and compliance tests to ensure portability of applications across the wide range of existing enterprise systems capable of supporting J2EE.

References:

Java Language Specification
http://java.sun.com/docs/books/jls/second_edition/html/j.title.doc.html

Java 2 Platform, Standard Edition Specification
http://java.sun.com/J2se/1.3/docs/index.html

Java 2 Platform, Micro Edition Specification
(taken from the FAWG E-Gov Guidance)
http://java.sun.com/J2me/docs/

Java Server Pages USP) Specification v1A
http://java.sun.com/products/ejb/docs.html

Java Virtual Machine Specification
http://java.sun.com/docs/books/vmspec/index.html

11 Microsoft Component Object Model (COM)

The Microsoft COM is a software architecture that allows applications to be built from binary software components. COM and COM+ are the basis for many Microsoft applications and APIs and are widely used and supported across the industry.

Reference: http://www.microsoft.com/com/resources/specs.asp

12 eXtensible Stylesheet Language (XSL)

XSL is a language for expressing style sheets that format the display and presentation of XML documents.

Reference: http://www.w3.org/Style/XSL/

13 Palm Operating System

Palm is the leading Personal Digital Assistant (PDA). Version 5 of Palm OS provides multitasking and other capabilities that will provide an improved platform for E-Gov. solutions.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.palmos.com/dev/

14 Blackberry

The leading email enabled wireless device with wide use in several Agencies.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.blackberry.com/developers/na/index.shtml

15 Symbian Epoc

A leading environment for web capable cellular phones.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.symbian.com/developer/index.html

16 WAP (Wireless Application Protocol)

The Wireless Application Protocol (WAP) is an open, global specification that empowers users of digital mobile phones, pagers, personal digital assistants and other wireless devices to securely access and interact with Internet/ Intranet/Extranet content, applications, and services.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.wapforum.org/

17 XHTMLMP (XHTML Mobile Profile)

XHTMLMP is designed for resource-constrained Web clients that do not support the full set of XHTML features, such as mobile phones, PDAs, pagers and set-top boxes. It extends XHTML Basic with modules, elements and attributes to provide a richer authoring language. XHTML replaces the Wireless Markup Language (WML).

Reference: (taken from the FAWG E-Gov Guidance)
http://www.wapforum.org/what/technical.htm

18 VXML (Voice XML)

VXML is an XML vocabulary for specifying IVR (Integrated Voice Response) Systems.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.w3c.org/Voice/
http://www.voicexml.org/

19 CC/PP - Composite Capability/Preference Profiles (emerging)

CC/PP framework specifies how client devices express their capabilities and references (the user agent profile) to the server that originates content (the origin server). The origin server uses the "user agent profile" to produce and deliver content appropriate to the client device. In addition to computer-based client devices, particular attention is being paid to other kinds of devices such as mobile phones.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.w3c.org/2001/di/

20 WebDAV (World Wide Web Distributed Authoring and Versioning)

WebDAV is an interface standard that defines the syntax used by an authoring tool when interacting with a Web server. It is a set of extensions to the I-ITTI? protocol, which allows users to collaboratively edit and manage files on remote web servers.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.webdav.org/
http://www.ietf.org/ids.by.wg/webdav.html

21 IMAP (RFC2060) V4.1 (Internet Message Access Protocol)

IMAP4rev1 allows a client to access and manipulate electronic mail messages on a server. IMAP4rev1 permits manipulation of remote message folders, called "mailboxes", in a way that is functionally equivalent to local mailboxes. IMAP4rev1 also provides the capability for an offline client to resynchronize with the server.

22 MIME (RFC 2045) (Multipurpose Internet Mail Extensions)

MIME extends the format of Internet mail to allow non-US- American Standard Code for Information Interchange (ASCII) textual messages, non-textual messages, multi-part message bodies, and non-US-ASCH information in message headers. MIME support allows compliant email clients and servers to accurately communicate embedded information to internal and external users.

23 T.120 - International Telecommunications Union (ITU)

T.120 contains a series of communication and application protocols and services that provide support for real-time, multipoint data communications. These multipoint facilities are important building blocks for collaborative applications, including desktop data conferencing, and multi-user applications.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.imtc.org/t120body.htm

24 H323 - International Telecommunications Union (ITU)

H.323 addresses Video (Audiovisual) communication on Local Area Networks, including Corporate Intranets and packet-switched networks generally.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.imtc.org/h323.htm

25 eXtensible Business Reporting Language (XBRL)

Extensible Business Reporting Language (XBRI) is an open specification, which uses XML-based data tags to describe financial statements for both public and private companies.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.xbrl.org/

26 SMTP (RFC821) (Simple Mail Transfer Protocol)

SMTP facilitates transfer of electronic-mail messages. It specifies how two systems are to interact, and the messages format used to control the transfer of electronic mail.

27 ESMTP (RFC1869) (Extended Simple Mail Transfer Protocol)

ESMTP allows new service extensions to SMTP to be defined and registered with Internet Assigned Numbers Authority (IANA)

28 Simple Network Management Protocol (SNMP V3)

SNMP V3 eliminates several of the security vulnerabilities in earlier version.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.ietf.org/rfc/rfc2570.txt?number=2570

29 Lightweight Directory Access Protocol - LDAP V3 (RFC 1779)

Lightweight Directory Access Protocol (LDAP) is a subset of X.500 designed to run directly over the TCP/IP stack. LDAP is, like X.500, both an information model and a protocol for querying and manipulating it. LDAPv3 is an update developed in the IETF (Internet Engineering Task Force), which addresses the limitations found during deployment of the previous version of LDAP.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.opengroup.org/directory/branding/1dap2000/x99di.htm

30 X.500 - International Telecommunication Union Telecommunication Standardization Sector (ITU)

Defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city.

31 ebXML - Electronic Business using XML

A modular suite of specifications that enables enterprises to conduct business over the Internet: exchanging business messages, conducting trading relationships, communicating data in common terms and defining and registering business processes.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.ebxml.org/

32 RDF (Resource Description Framework)

RDF provides a lightweight ontology system to support the exchange of knowledge on the Web. It integrates a variety of web-based metadata activities including sitemaps, content ratings, stream channel definitions, search engine data collection (web crawling), digital library collections, and distributed authoring, using XML as interchange syntax. RDF is the foundation for the Semantic Web envisioned by Tim Berners-Lee - an extension of the current web in which information is given well-defined meaning, better enabling computers and people to work in cooperation.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.w3.org/RDF/
http://www.w3.org/2001/sw/

33 Web Content Accessibility Guidelines 1.0, W3C

Provides guidelines on how to design and develop web pages that meet accessibility guidelines.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.w3.org/WAI/
http://www.w3.org/TR/WCAG10/

34 DAML+Oll, (Defense Advanced Research Projects Agency (DARPA) Agent Modeling Language + Ontology Inference Layer)

DAML+OlL is a semantic markup language for Web resources to allow automated systems to understand the meaning of information even when different terms are used for the same concept. It builds on earlier W3C standards such as RDI` and RDF Schema, and extends these languages with richer modeling primitives.

Reference: (taken from the FAWG E-Gov Guidance)
http://www.w3.org/TR/daml+oil-reference

35 DoD 5015.2-STD (Department of Defense, Design Criteria Standard for Electronic Records Management Software Applications)

Reference: (taken from the FAWG E-Gov Guidance)
http://www.dtic.mil/whs/directives/corres/html/50152std.htm

36 IS015489 (International Standards Organization Records Management Standard)

Reference: (taken from the FAWG E-Gov Guidance)
http://www.iso.org/iso/en/ISOOnline.frontpage

Appendix G – Service Domains, Service Types and Components

Customer Services Domain

The Customer Services Domain defines the set of capabilities that are directly related to an internal or external customer, the business' interaction with the customer, and the customer driven activities or functions. The Customer Services domain represents those capabilities and services that are at the front end of a business, and interface at varying levels with the customer.

Customer Relationship Management - defines the set of capabilities that are used to plan, schedule and control the activities between the customer and the enterprise both before and after a product or service is offered.

Call Center Management - defines the set of capabilities that handle telephone sales and/or service to the end customer.

Customer Analysis - defines the set of capabilities that allow for the analysis of an organization's customers as well as the scoring of third party information as it relates to an organization's customers.

Sales and Marketing - defines the set of capabilities that facilitate the promotion of a product or service and capture of new business.

Product Management - defines the set of capabilities that facilitate the creation and maintenance of products and services.

Brand Management – defines the set of capabilities that support the application of a trade name to a product or service as well as developing awareness for the name.

Customer/Account Management – defines the set of capabilities that support the retention and delivery of a service or product to an organization's clients.

Contact Management – defines the set of capabilities that keep track of people and the related activities of an organization.

Partner Relationship Management – defines the set of capabilities that are used to plan and control the activities between an organization, its stakeholders and business partners, including third parties that support services to an organization's stakeholders.

Customer Feedback – defines the set of capabilities that are used to collect, analyze and handle comments and feedback from an organization's customers.

Surveys - defines the set of capabilities that are used to collect useful information from an organization's customers.

Customer Preferences - defines the set of capabilities that allow an organization's customers to change a user interface and the way that data is displayed.

Personalization – defines the set of capabilities to change a user interface and how

data is displayed.

Subscriptions – defines the set of capabilities that allow a customer to join a forum, listserv, or mailing list.

Alerts and Notifications – defines the set of capabilities that allow a customer to be contacted in relation to a subscription or service of interest.

Profile Management – defines the set of capabilities that allow for the maintenance and modification of a customer's account information related to their profile.

Customer Initiated Assistance - defines the set of capabilities that allow customers to proactively seek assistance and service from an organization.

Online Help – defines the set of capabilities that provide an electronic interface to customer assistance.

Online Tutorials – defines the set of capabilities that provide an electronic interface to educate and assist customers.

Self-Service – defines the set of capabilities that allow an organization's customers to sign up for a particular service at their own initiative.

Reservations / Registration – defines the set of capabilities that allow electronic enrollment and confirmations for services.

Multi-Lingual Support – defines the set of capabilities that allow access to data and information in multiple languages.

Assistance Request - defines the set of capabilities that support the solicitation of support from a customer.

Scheduling - defines the set of capabilities that support the plan for performing work or service to meet the needs of an organization’s customers.

Process Automation Services Domain

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

Tracking and Workflow - defines the set of capabilities for automatic monitoring and routing of documents to the users responsible for working on them to support each step of the business cycle.

Process Tracking – defines the set of capabilities to allow the monitoring of activities within the business cycle.

Case/Issue Management – defines the set of capabilities for managing the life cycle of a particular claim or investigation within an organization to include creating, routing,

tracing, assignment and closing of a case as well as collaboration among case handlers.

Conflict Resolution – Defines the set of capabilities that support the conclusion of contention or differences within the business cycle.

Routing and Scheduling - defines the set of capabilities for the automatic directing, assignment, or allocation of time for a particular action or event.

Inbound Correspondence Management – defines the set of capabilities for the management of externally initiated communication between an organization and its stakeholders.

Outbound Correspondence Management – defines the set of capabilities for the management of internally initiated communication between an organization and its stakeholders.

Business Management Services Domain

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

Management of Process - defines the set of capabilities that regulate the activities surrounding the business cycle of an organization.

Change Management – defines the set of capabilities that control the process for updates or modifications to the existing documents, software or business processes of an organization.

Configuration Management – defines the set of capabilities that control the hardware and software environments, as well as documents of an organization.

Requirements Management – defines the set of capabilities for gathering, analyzing and fulfilling the needs and prerequisites of an organization's efforts.

Program/Project Management – defines the set of capabilities for the management and control of a particular effort of an organization.

Governance / Policy Management – defines the set of capabilities intended to influence and determine decisions, actions, business rules and other matters within an organization.

Quality Management - defines the set of capabilities intended to help determine the level of assurance that a product or service will satisfy certain requirements.

Business Rule Management – defines the set of capabilities for the management of the enterprise processes that support an organization and its policies.

Risk Management – defines the set of capabilities that support the identification and probabilities or chances of hazards as they relate to a task, decision or long-term goal.

Organizational Management – defines the set of capabilities that support both collaboration and communication within an organization.

Workgroup/Groupware - defines the set of capabilities that support multiple users working on related tasks.

Network Management - defines the set of capabilities involved in monitoring and maintaining a communications network in order to diagnose problems, gather statistics and provide general usage.

Investment Management - defines the set of capabilities that manage the financial assets and capital of an organization.

Strategic Planning & Mgmt – defines the set of capabilities that support the determination of long-term goals and the identification of the best approach for achieving those goals.

Portfolio Management – defines the set of capabilities that support the administration of a group of investment held by an organization.

Performance Management - defines the set of capabilities for measuring the effectiveness of an organization's financial assets and capital.

Supply Chain Management - defines the set of capabilities for planning, scheduling and controlling a supply chain and the sequence of organizations and functions that mine, make or assemble materials and products from manufacturer to wholesaler to retailer to consumer.

Procurement - defines the set of capabilities that support the ordering and purchasing of products and services.

Sourcing Management – defines the set of capabilities that support the supply of goods or services as well as the tracking and analysis of costs for these goods.

Catalog Management – defines the set of capabilities that support the listing of available products or services that an organization offers.

Ordering/Purchasing – defines the set of capabilities that allow the placement of request for a product.

Invoice/Requisition Tracking and Approval – defines the set of capabilities that support the identification of where a shipment or delivery is within the business cycle.

Storefront/Shopping Cart - defines the set of capabilities that support the online equivalent of the supermarket cart, where orders and merchandise are placed.

Returns Management – defines the set of capabilities for collecting, analyzing, and resolving product returns or service cancellations.

Digital Asset Services Domain

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

Content Management – defines the capabilities that manage the storage, maintenance and retrieval of documents and information of a system or website.

Content Authoring – defines the capabilities that allow for the creation of tutorials, CBT courseware, Web sites, CD-ROMs and other interactive programs.

Content Review and Approval – defines the capabilities that allow for the approval of interactive programs.

Tagging and Aggregation – defines the set of capabilities that support the identification of specific content within a larger set of content for collection and summarization.

Content Publishing and Delivery – defines the set of capabilities that allow for the propagation of interactive programs.

Syndication Management - defines the set of capabilities that control and regulate an organization's brand.

Document Management – defines the set of capabilities that control the capture and maintenance of an organization's documents and files.

Document Imaging and OCR – defines the set of capabilities that support the scanning of physical documents for use electronically.

Document Referencing – defines the set of capabilities that support the re-direction to other documents and information for related content.

Document Revisions – defines the set of capabilities that support the versioning and editing of content and documents.

Library/Storage – defines the set of capabilities that support document and data warehousing and archiving.

Document Review and Approval – defines the set of capabilities that support the editing and commendation of documents before releasing them.

Document Conversion – defines the set of capabilities that support the changing of files from one type of format to another.

Indexing – defines the set of capabilities that support the rapid retrieval of documents through a structured numbering construct.

Classification – defines the set of capabilities that support the categorization of documents.

Knowledge Management - defines the set of capabilities that support the identification, gathering and transformation of documents, reports and other sources into meaningful information.

Information Retrieval – defines the set of capabilities that allow access to data and information for use by an organization and its stakeholders.

Information Mapping/Taxonomy – defines the set of capabilities that support the creation and maintenance of relationships between data entities, naming standards and categorization.

Information Sharing – defines the set of capabilities that support the use of documents and data in a multi-user environment for use by an organization and its stakeholders.

Categorization – defines the set of capabilities that allow classification of data and information into specific layers or types to support an organization.

Knowledge Engineering – defines the set of capabilities that support the translation of knowledge from an expert into the knowledge base of an expert system.

Knowledge Capture – defines the set of capabilities that facilitate collection of data and information.

Knowledge Discovery - defines the set of capabilities that facilitate the identification of useful information from data.

Knowledge Distribution and Delivery - defines the set of capabilities that support the transfer of knowledge to the end customer.

Records Management - defines the set of capabilities to support the storage, protection, archiving, classification and retirement of documents and information.

Record Linking / Association - defines the set of capabilities that support the correlation between logical data and information sets.

Document Classification – defines the set of capabilities that support the categorization of documents and artifacts, both electronic and physical.

Document Retirement – defines the set of capabilities that support the termination or cancellation of documents and artifacts used by an organization and its stakeholders.

Digital Rights Management – defines the set of capabilities that support the claim and ownership of intellectual capital and artifacts belonging to an organization.

Business Analytical Services Domain

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

Analysis and Statistics - defines the set of capabilities that support the examination of business issues, problems and their solutions.

Modeling – defines the set of capabilities that support the simulating of conditions or activities by performing a set of equations on a set of data.

Predictive – defines the set of capabilities that support the foretelling of something in advance by the use of data.

Simulation – defines the set of capabilities that support the representation of the interaction between real-world objects.

Mathematical – defines the set of capabilities that support the use of mathematical functions and algorithms for the analysis of data.

Structural / Thermal – defines the set of capabilities that support the use of data flow and data modeling diagrams for applying systematic analysis of data.

Radiological – defines the set of capabilities that support the use of radiation and x-ray technologies for analysis and scientific examination.

Forensics – defines the set of capabilities that support the analysis of physical elements using science and technology for investigative and legal purposes.

Visualization - defines the set of capabilities that support the conversion of data into graphical or picture form.

Graphing / Charting – defines the set of capabilities that support the presentation of information in the form of diagrams or tables.

Imagery – defines the set of capabilities that support the creation of film or electronic images from pictures, paper forms or graphics for static or dynamic use.

Multimedia – defines the set of capabilities that support the representation of information in more than one form to include text, audio, graphics, animated graphics and full motion video.

Mapping / Geospatial / Elevation / GPS – defines the set of capabilities that support the use of elevation, latitude and longitude coordinates.

CAD - defines the set of capabilities that support the design of products with computers.

Business Intelligence - defines the set of capabilities that support information that pertains to the history, current status or future projections of an organization.

Demand Forecasting / Mgmt – defines the set of capabilities that facilitate the prediction of sufficient production to meet an organization's sales of a product or service.

Balanced Scorecard – defines the set of capabilities that support the listing and analyzing of both positive and negative impacts associated with a decision.

Decision Support and Planning – defines the set of capabilities that support the analysis of information and predict the impact of decisions before they are made.

Data Mining - defines the set of capabilities that support the exploring and analyzing of detailed business transactions to uncover patterns and relationships within the business activity and history.

Reporting - defines the set of capabilities that support the organization of data into useful information.

Ad Hoc – defines the set of capabilities that support the use of dynamic reports on an as needed basis.

Standardized/Canned – defines the set of capabilities that support the use of pre-conceived or pre-written reports.

OLAP - defines the set of capabilities that support the analysis of information that has been summarized into multidimensional views and hierarchies.

Back Office Services Domain

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

Data Management - defines the set of capabilities that support the usage, processing and general administration of unstructured information.

Data Exchange – defines the set of capabilities that support the interchange of information between multiple systems or applications.

Data Mart – defines the set of capabilities that support a subset of a data warehouse for a single department or function within an organization.

Data Warehouse – defines the set of capabilities that support the archiving and storage of large volumes of data.

Meta Data Management – defines the set of capabilities that support the maintenance and administration of data that describes data.

Data Cleansing – defines the set of capabilities that support the removal of incorrect or unnecessary characters and data from a data source.

Extraction and Transformation – defines the set of capabilities that support the manipulation and change of data.

Loading and Archiving – defines the set of capabilities that support the population of a data source with external data.

Data Recovery – defines the set of capabilities that support the restoration and stabilization of data sets to a consistent, desired state.

Data Classification – defines the set of capabilities that allow the classification of data.

Human Resources - defines the set of capabilities that support the recruitment and management of personnel.

Recruiting – defines the set of capabilities that support the identification and hiring of employees for an organization.

Resume Management – defines the set of capabilities that support the maintenance and administration of one's professional or work experience and qualifications.

Career Development and Retention – defines the set of capabilities that support the monitoring of performance as well as the professional growth, advancement, and retention of an organization's employees.

Time Reporting – defines the set of capabilities that support the submission, approval and adjustment of an employee's hours.

Awards Management – defines the set of capabilities that support the recognition of achievement among employees of an organization.

Benefit Management – defines the set of capabilities that support the enrollment and participation in an organization's compensation and benefits programs.

Retirement Management - defines the set of capabilities that support the payment of benefits to retirees.

Personnel Administration –defines the set of capabilities that support the matching between an organization's employees and potential opportunities as well as the modification, addition and general upkeep of an organization's employee-specific information.

Education/Training - defines the set of capabilities that support the active building of employee capacities.

Health and Safety – defines the set of capabilities that support the security and physical well-being of an organization's employees.

Travel Management – defines the set of capabilities that support the transit and mobility of an organization's employees for business purposes.

Financial Management - defines the set of capabilities that support the accounting practices and procedures that allow for the handling of revenues, funding and expenditures.

Billing and Accounting – defines the set of capabilities that support the charging, collection and reporting of an organization's accounts.

Credit / Charge – defines the set of capabilities that support the use of credit cards or electronic funds transfers for payment and collection of products or services.

Expense Management – defines the set of capabilities that support the management and reimbursement of costs paid by employees or an organization.

Payroll – defines the set of capabilities that involve the administration and determination of employees' compensation.

Payment/Settlement – defines the set of capabilities that support the process of accounts payable.

Debt Collection – defines the set of capabilities that support the process of accounts receivable.

Revenue Management – defines the set of capabilities that support the allocation and re-investment of earned net credit or capital within an organization.

Auditing – defines the set of capabilities that support the examination and verification of records for accuracy.

Activity – Based Management – defines the set of capabilities that support a defined, specific set of finance-related tasks for a given objective.

Currency Translation - defines the set of capabilities that support the calculations and differences among multiple mediums of exchange.

Financial Reporting - defines the set of capabilities that support the structured dissemination of financial data and information in both physical format and electronic media.

Assets/Materials Management – defines the set of capabilities that support the acquisition, oversight and tracking of an organization's assets.

Property/Asset Management – defines the set of capabilities that support the identification, planning and allocation of an organization's physical capital and resources.

Asset Cataloging / Identification – defines the set of capabilities that support the listing and specification of available assets.

Asset Transfer, Allocation, and Maintenance – defines the set of capabilities that support the movement, assignment, and replacement of assets.

Facilities Management – defines the set of capabilities that support the construction, management and maintenance of facilities for an organization.

Computers/Automation Management – defines the set of capabilities that support the identification, upgrade, allocation and replacement of physical devices, including servers and desktops, used to facilitate production and process-driven activities.

Development and Integration - defines the set of capabilities that support the communication between hardware/software applications and the activities associated with deployment of software applications.

Legacy Integration – defines the set of capabilities that support the communication between newer generation hardware/software applications and the previous, major generation of hardware/software applications.

Enterprise Application Integration – defines the set of capabilities that support the redesigning of disparate information systems into one system that uses a common set of data structures and rules.

Data Integration - defines the set of capabilities that support the organization of data from separate data sources into a single source using middleware or application integration as well as the modification of system data models to capture new information within a single system.

Instrumentation and Testing – defines the set of capabilities that support the validation of application or system capabilities and requirements.

Software Development –defines the set of capabilities that support the creation of both graphical and process application or system software.

Human Capital/Workforce Management – defines the set of capabilities that support the planning and supervision of an organization’s personnel.

Resource Planning and Allocation – defines the set or capabilities that support the means for assignment of employees and assets to sustain or increase an organization's business.

Skills Management – defines the set of capabilities that support the proficiency of employees in the delivery of an organization's products or services.

Workforce Directory/Locator – defines the set of capabilities that support the listing of employees and their whereabouts.

Team/Org Management – defines the set of capabilities that support the hierarchy structure and identification of employees within the various sub-groups of an organization.

Contingent Workforce Management – defines the set of capabilities that support the continuity of operations for an organization's business through the identification of alternative organization personnel.

Workforce Acquisition/Optimization - defines the set of capabilities that support the hiring and re-structuring of employees and their roles within an organization.

Support Services Domain

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

Security Management – defines the set of capabilities that support the protection of an organization's hardware/software and related assets.

Identification and Authentication – defines the set of capabilities that support obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users.

Access Control – defines the set of capabilities that support the management of permissions for logging onto a computer or network.

Encryption – defines the set of capabilities that support the encoding of data for security purposes.

Intrusion Detection – defines the set of capabilities that support the detection of illegal entrance into a computer system.

Verification – defines the set of capabilities that support the confirmation of authority to enter a computer system, application or network.

Digital Signature – defines the set of capabilities that guarantee the unaltered state of a file.

User Management – defines the set of capabilities that support the administration of computer, application and network accounts within an organization.

Role/Privilege Management - defines the set of capabilities that support the granting of abilities to users or groups of users of a computer, application or network.

Audit Trail Capture and Analysis – defines the set of capabilities that support the identification and monitoring of activities within an application or system.

Collaboration – defines the set of capabilities that allow for the concurrent, simultaneous communication and sharing of content, schedules, messages and ideas within an organization.

Email - defines the set of capabilities that support the transmission of memos and messages over a network.

Threaded Discussions – defines the set of capabilities that support the running log of remarks and opinions about a given topic or subject.

Document Library – defines the set of capabilities that support the grouping and archiving of files and records on a server.

Shared Calendaring – defines the set of capabilities that allow an entire team as well as individuals to view, add and modify each other's schedules, meetings and activities.

Task Management – defines the set of capabilities that support a specific undertaking or function assigned to an employee.

Search - defines the set of capabilities that support the probing and lookup of specific data from a data source.

Query – defines the set of capabilities that support retrieval of records that satisfy specific query selection criteria.

Precision / Recall Ranking – defines the set of capabilities that support selection and retrieval of records ranked to optimize precision against recall.

Classification – defines the set of capabilities that support selection and retrieval of records organized by shared characteristics in content or context.

Pattern Matching – defines the set of capabilities that support retrieval of records generated from a data source by imputing characteristics based on patterns in the content or context.

Communication - defines the set of capabilities that support the transmission of data, messages and information in multiple formats and protocols.

Real Time/Chat – defines the set of capabilities that support the conferencing capability between two or more users on a local area network or the internet.

Instant Messaging – defines the set of capabilities that support keyboard conferencing over a Local Area Network or the internet between two or more people.

Audio Conferencing – defines the set of capabilities that support audio communications sessions among people who are geographically dispersed.

Video Conferencing – defines the set of capabilities that support video communications sessions among people who are geographically dispersed.

Event/News Management – defines the set of capabilities that monitor servers, workstations and network devices for routine and non-routine events.

Community Management - defines the set of capabilities that support the administration of online groups that share common interests.

Computer/Telephony Integration - defines the set of capabilities that support the connectivity between server hardware, software and telecommunications equipment into a single logical system.

Systems Management – defines the set of capabilities that support the administration and upkeep of an organization's technology assets, including the hardware, software, infrastructure, licenses and components that comprise those assets.

License Management – defines the set of capabilities that support the purchase, upgrade and tracking of legal usage contracts for system software and applications.

Remote Systems Control – defines the set of capabilities that support the monitoring, administration and usage of applications and enterprise systems from locations outside of the immediate system environment.

System Resource Monitoring – defines the set of capabilities that support the balance and allocation of memory, usage, disk space and performance on computers and their applications.

Software Distribution – defines the set of capabilities that support the propagation, installation and upgrade of written computer programs, applications and components.

Forms Management – defines the set of capabilities that support the creation, modification and usage of physical or electronic documents used to capture information within the business cycle.

Forms Creation – defines the set of capabilities that support the design and generation of electronic or physical forms and templates for use within the business cycle by an organization and its stakeholders.

*Forms Modification - d*efines the set of capabilities that support the maintenance of electronic or physical forms, templates and their respective elements and fields.

Appendix H - Priority Service and Transformation outcome for MDAs

INTRODUCTION:

Linking MDA e-government investment to the delivery of service improvement in shared priority areas serves to address the real concerns of citizens, as well as providing a focus for Sector Ministries and their departments and agencies up to the 2007 target and beyond.

A key objective of the e-government office involves improving delivery and value for money of services within a framework of national policies and targets. This includes assisting MDAs to achieve 100% capability in electronic delivery of priority services by 2007 in ways that citizens and business will use.

In order to define what is meant by the term “priority services” and for the Government to measure progress towards the Public Service Agreement (PSA) target, it is necessary to agree a set of e-government priority outcomes for each MDA. Furthermore, it is expected that each MDA as part of its e-government investment programme will deliver these priority outcomes by December 2007.

The proposed priority outcomes will be derived primarily from the shared priorities agreed by the e-government office with the MDAs. For practical purposes, the shared priorities will be translated into a set of priority service and transformation areas. The MDAs are expected to be delivered the proposed outcomes by December 2007. The proposed priority outcomes provide a focus for priority working within the e-government office target to reach 100% e-enablement of Government Services by December 2007.

About the proposed approach to defining priority outcomes

The proposed approach to priority outcomes outlined in this document is designed to provide:

(i) clarity to citizens and business regarding what they can expect to be able to do electronically with the MDAs,

(ii) a leap forward from the existing manual delivery of services around a general “e-enablement” of services based around clearer deliverables under the shared priorities for better MDAs service delivery.

The proposed approach is also designed to:

(iii) demonstrate the link between National Strategy and the Ghana Poverty Reduction Strategy (GPRS) for the MDAs;

(iv) allow local authorities scope to map the proposed list of priority outcomes within a three year time frame;

(v) provide an operational focus for the MDAs programme in terms of the 2007 target;

(vi) raise awareness about the work of National Projects and their potential contribution to priority service objectives and

(i) provide a platform for the adoption of e-government as a key issue for assessing the performance of the MDAs assessment.

Partnerships

Whilst it is at the discretion of MDAs whether they wish to deliver the priority outcomes by working individually, or through partnerships, there is a strong expectation that existing partnership infrastructures represent a preferred way forward to deliver outcomes in priority areas that demand an integrated or joined-up approach.

Outcomes

The proposed outcomes for each priority service and transformation area are defined in terms of:

(vii) **Best practice outcomes** – all MDAs are expected to have the named outcomes in place for each priority area by the end of December 2007

(viii) **Mandatory outcomes** – these refer to specific online facilities that must be in place in every area of the country for citizens, business, organizations, councilors, traditional chiefs and local authority staff to use by the end of December 2007

(i) **Discretionary outcomes** - high performing MDAs that have already achieved or largely achieved, the defined best practice and mandatory outcomes, will be given the discretion to establish their own targets for how they wish to further develop services to deliver sustainable e-government up to 2007 and beyond.

MODEL EXAMPLE FOR THE PROPOSED PRIORITY AREAS AND OUTCOMES.

PRIORITY SERVICE AREA	PROPOSED OUTCOMES
(1) Community Information To deliver integrated services for the citizens, business and local partnerships where appropriate, and connected to a national infrastructure. **Shared Service/National Priority** (i) creating safer and stronger communities (ii) promoting healthier communities and narrowing health inequalities (iii) supporting the economic vitality of district assemblies. **Associated National Projects** (i) Community Based Poverty Reduction Project-Street Children (CPRP). (ii) Agricultural Services Sub-Sector Investment Programme (AgSSIP)	1) **Best practice outcomes** in 2007 to include: • Fulfillment of national standards on accessibility and interoperability • Development of systems to help local authority to understand their local housing market and to inform work on balancing housing markets (i.e. supply versus demand) 2) **Mandatory outcomes** – online facilities to be available to allow: • Development of shared community information databases linked to the delivery of services via community portals and or contract centre to enable a single point of access to a wide and comprehensive range of community information. • Provision of information on fire safety • Application to join housing register.

PRIORITY SERVICE AREA	PROPOSED OUTCOMES
(2) Environmental Quality To use technology to integrate relevant functions more closely and help improve the quality cleanliness and safety of our public space Shared Service/National Priority: • transforming our local environment • creating safer and stronger communities • e-planning Associated National Projects • Planning & Regulatory Services Online (PARSOL) • Knowledge Management	**(1) Best Practice outcomes** in 2007 to include: • Implementation of systems to integrate and support coordinated activity across the public sector and civil service (i.e. the police, NADMO, fire etc.) designed to manage the physical clean, green and safe public space; • Evidence of improvement in the % of people satisfied with the cleanliness standard in their area • Establishment of information architecture to provide contact to 'Home & Community' franchise of the Online Governments • Use of Geographical Information System (GIS) for map-based data presentation of property-related information (2) **Mandatory outcomes** – Online facilities to be available to allow transaction in respect of: • E-enabled reporting/applications, procurement and projects chasing of environmental services, includes waste management and street scene (e.g. abandoned cars, bulky waste removal, recycling); • Receipt and processing of planning and building control applications; • Submission and tracking of regulation and licensing services. **(3) Discretionary outcomes** – target to be defined by high performing Districts Assemblies

PRIORITY SERVICE AREA	PROPOSED OUTCOMES
	• Development of online facilities for interactive computer simulation of issues affecting environmental quality.
(3) e-Procurement Supporting business improvement through cost effective and efficient purchasing of goods and services through MDAs implementation of e-procurement. Working with local suppliers to equip them to take advantage of e-procurement activities shared services. **Shared Service/National Priority** • Procurement Bill • Public Financial Management Reform Programme (PURMARP)	**(1) Best practice outcomes** in 2007 to include: • Inclusion of Small and Medium Enterprises (SMEs) in e-procurement programme • Promote the advantages of e-procurement to local suppliers and retain development benefits within local community • Demonstration of efficiency savings by December 2007 including improvement in the % of undisputed invoices paid within 3 days • Co-operate on e-procurement between MDAs **(2) Mandatory outcomes** – online facilities to be available to allow: • Online publication of selling to the MDAs; • Appropriate e-procurement solutions in place, including paperless ordering, invoices and payment; • Establishment of a single business account. **(3) Discretionary outcomes** – target to be defined by high performing MDAs e.g. • Access to virtual e-procurement marketplace' established; • Services for suppliers to

PRIORITY SERVICE AREA	PROPOSED OUTCOMES
	include e-mails and SMS text messaging (e.g. to notify business to quote and tender for MDAwork)
4) Supporting new ways of working Active policy and practice enabling Civil and Public Servants to work from home or away from the office base Shared Service/National Priority; -office of e-government National Strategy Associated National Projects -Government Wide Area Network	**(i) Best Practice outcomes** in 2007 to include: • ICT Support and documented policy for home working (tele-working) for Senior Civil and Public Servants. • E-mail and Internet access provided for senior staff • Establishment of e-skills training programme for Senior, Middle and Junior staff (i) **Mandatory outcomes** – online facilities to be available to allow: • Secure remote access to MDA systems including Intranet • Access to home working facilities to all Civil & Public servants by the MDAs published home working policy (ii) **Discretionary outcomes** – target to be defined by high performing MDAs, e.g. • Provision of mobile technology to support MDAs service delivery Establishment of "drop in centres" to enable staff to work closer to home.
(5) Accessibility of Services	

PRIORITY SERVICE AREA	PROPOSED OUTCOMES
All MDA services are available outside of standard working hours via the Internet or "KIOSK"/centres Shared Service/National Priority **(6) Making it easy for citizens and business to do business with the MDAs. Systems are in place to ensure effective customer relationship management.**	**(1) Best practice outcomes** in 2007 to include: • 100% e-enablement of services in line with 2007 target • 80% of public enquires about MDAs services resolved at the first point of contact • All MDAs services are available outside standard working hours via the Internet or telephone contact centres (i.e. available for extended hours outside of 9am-5pm Monday to Friday) • Compliance with freedom of Information Act requirements **(2) Mandatory outcomes** – online facilities to be available to allow: • Conformance with Web Accessibility initiative standards on website accessibility • Compliance with government Interoperability Framework including Metadata standard • Access to service A-Z detailing service availability for all public services **(3) Discretionary outcomes** – target to be defined by high performing MDAs, e.g. • 24/7 access to services via a telephone contact centre where there is a defined emergency need.

PRIORITY SERVICE AREA	PROPOSED OUTCOMES
Shared Service/National Priority • Ghana Poverty Reduction Strategy (GPRS) Lands Adm. Project (LAP) **Associated National Projects** • Working with business • Work flow • Records Documents Information Management Systems (RDIMS)	1) **Best practice outcome** in 2007 to include: • Systems in place to ensure effective and consistent customer relationship management across access channels and to provide a first time fix for customer enquires, i.e. using a common database, which holds customers records, to deliver services across different channels, and enabling joined-up and automated service delivery • Establishment of simple accounts for citizens and business • Compliance with spatial datasets (BS7666) for geographical referencing for unambiguous identification of land and property. 2) **Mandatory outcomes** – online facilities to be available to allow: • Automated e-mail acknowledgement of all public enquires received via government websites or regional portals. • Publication of service standards for customer enquires received via e-mail or web form • Sign-up facility to enable citizens or business to be contacted via e-mail

PRIORITY SERVICE AREA	PROPOSED OUTCOMES
	or SMS text message for services that they request to be notified about. 3) **Discretionary outcomes** – targets to be defined by high performing MDAs, e.g. • Integration of RDIMS with back office activity through use of enabling technology such as workflow to create complete automation of business process management.

The above model examples for the proposed priority service /transformation areas and proposed outcomes should be used by the MDAs including best practices, mandatory and discretionary outcomes, as a guide in developing their business e-government frontline services.

A partial list of frontline e-government services by Sector Ministries and their departments and agencies is provided below as a reference point in the development and implementation process.

E-Government Services

INITIATIVE	MDA's	SERVICES/TRANSFORMATION AREAS.
Services	Ministry of Justice & Attorney General's Dept.	The Ministry of Justice Database and Information System will provide data on the following: (i) Passed bills and statutes (ii) Business Permit & registration etc. (iii) On-line bidding (iv) Profile of private & NGO's within their sector
Services	Ministry of Foreign Affairs	The Ministry of Foreign Affairs Database & Information System will provide: (i) all our Embassies on business opportunities; (ii) tourism; (iii) on-line application for passport; (iv) Directory, website & locations of foreign Missions in Ghana;

INITIATIVE	MDA's	SERVICES/TRANSFORMATION AREAS.
		(v) Requirements for entry to other countries, etc., (vi) On-line bidding (vii) profile of private & NGO's within their sector
Services	Ministry of Roads & Transport	The Ministry of Roads & Transport Database and Information System will provide: (i) On-line vehicle registration (ii) Drivers licensing (iii) Vehicles profile (iv) On-line bidding (v) Profile of private & NGO's within their sector
Services	Ministry of Interior	The Ministry of Interior Database and Information System will provide: (i) Crime and disaster report (ii) Permits for work and residency; (iii) Dual citizenship (iv) Registration of private security agencies; (v) On-line bidding Profile of private & NGO within their sector
Services	Office of the President	The Office of the President Executive Information System will provide: (i) MDA's with the facility to report to the President (ii) Monitoring the implementation of Govt. policies & feedback from the Central Management Agencies (CMA's) & the public.
Services	Ministry of Education, Youth and Sports	The Ministry of Education, Youth & Sports Database and Information System will provide: (i) Education Statistics (ii) Performance ranking of the second cycle institutions (iii) Subject areas (specialization); (iv) Educational facilities; (v) Scholarships Directory; (vi) Approved fees; (vii) Tertiary Institutions & programmes (viii) On-line bidding (ix) Profile of private & NGO's within their sector

INITIATIVE	MDA's	SERVICES/TRANSFORMATION AREAS.
Services	Ministry of Trade, Industry and PSI	The Ministry of Trade, Industry & PSI Database and Information System will provide: (i) information on the industrial sector; (ii) Products standards for export (iii) industrial performance and statistics; (iv) List of planning & ongoing PSI programmes (v) On-line bidding (vi) Profile of private 7 NGO's within their sector
Services	Ministry of Food & Agriculture	The Ministry of Food & Agriculture Database and Information System will provide: (i) market prices and other locations of bumper harvest; (ii) internal & external markets (iii) Products standard for export. (iv) On-line bidding (v) Profile of private & NGO's within their sector
Services	Ministry of Health	The Ministry of Health Database and Information System will provide: (i) health facilities; (ii) doctor/nurse patient ratios; (iii) health ranking; (iv) health statistics; (v) On-line bidding; (vi) Profile of private & NGO's within their sector
Services	Ministry of Lands & Forestry	The Ministry of Lands & Forestry Database and Information System will provide: (i) Landownership; (ii) Land prices & location; (iii) Land registration & titling; (iv) Seedlings & aforestation programmes; (v) On-line bidding (vi) Profile of private & NGO's within their sector

INITIATIVE	MDA's	SERVICES/TRANSFORMATION AREAS.
Services	Ministry of Manpower Development and Employment	The Ministry of Manpower Development and Employment Database and Information System will provide: (i) labour statistics ; (ii) employment opportunities; (iii) training for the physically challenged; (iv) On-line bidding (v) profile of private & NGO's within their sector
Services	Ministry of Works & Housing	The Ministry of Works and Housing Database and Information System will provide: (i) Information on all Govt. properties and costs (ii) On-line bidding (iii) profile of private & NGO's within their sector
Services	Ministry of Local Government and Rural Development	The Local Government &Rural Development Database and Information System will provide: (i) the percentage breakdown of the common fund; (ii) the Internal Generated Fund(IGF) for socio-economic development in the districts; (iii) the number of second cycle, tertiary institutions & their ranking; (iv) location of health facilities; (v) doctor/nurse patient ratios; (vi) socio-economic ranking of the districts, (vii) birth and death certificates; (viii) list of approved projects (ix) On-going & completed common fund projects. (x) On-line bidding (xi) Profile of private & NGO's within their sector (xii) Profile of environmental and sanitation issues.
Services	Ghana Statistical Service	The Ghana Statistical Service Database and Information System will provide: (i) National, Regional &

INITIATIVE	MDA's	SERVICES/TRANSFORMATION AREAS.
		district socio-economic data; (ii) housing statistics; (iii) poverty & demography statistics; (iv) Local housing & income statistics; (v) On-line bidding (vi) Profile of private & NGO's within their sector
Services	Ministry of Private Sector Development	The Ministry of Private Sector Development Database and Information System will provide: (i) Sources of credit for businesses, etc. (ii) On-line bidding (iii) profile of private & NGO's within the sector
Services	Ministry of Regional Co-operation and NEPAD	The Ministry of Regional Co-operation and NEPAD Database and Information System will provide: (i) Regional protocols and the stages of implementation. (ii) On-line bidding (iii) Profile of private & NGO's within their sector
Services	Office of the Head of Civil Service	The Integrated Personnel & Payroll Database (IPPD) system will provide manpower statistics, cost and personnel profile. (i) On-line bidding (ii) Profile of MDA's, private & NGO's organization.
Service	Ministry of Finance & Economic Planning	The Ministry of Finance & Economic Planning Database and Information will provide: (i) value for money prices (ii) budget details and budget performance (iii) statistics on budget, expenditures, revenue, inventories, maintenance and utilization, deployment and distribution; (iv) VAT Returns & Invoices (v) Corporate income tax (vi) Tax returns & notices (vii) Tax Collection (viii) Custom declaration, (ix) CAP30 & Social Security benefits.

INITIATIVE	MDA's	SERVICES/TRANSFORMATION AREAS.
		(x) On-line bidding Private of private & NGO's within their sector

Appendix I - Programme Management Documents

Documents to be developed for the implementation of the strategy include

- National Program for Implementation of E-government
- Action Plan for the Implementation of the Strategy
- Terms of reference for the development of a Management Information System for the management of the E-Government development process
- Project Management Methodology (national, interdepartmental and institutional)
- Methodology for the Management of Procurement and Services Contracts
- Information Security Policy
- Rules and Procedures for Interdepartmental Information Exchange
- Architectures and Requirements for Information Systems in the Public
- Administration

Appendix J – Practical Considerations for MDA E-Government Implementation

Introduction

This appendix focuses on the practical considerations each MDA needs to make in implementing an e-government solution.

As indicated in Section XX there are a number of steps in adopting the Government's Enterprise Architecture.

These will require that each MDA evaluate its readiness to embrace e-government. The following questions will help in this regard. These questions are by no means exhaustive, but should be regarded as a tool to help determine what an institution is ready to do with regard to adopting the government's e-government strategy and should guide the process of determining how this is done.

Evaluate the organizations Web Presence

What services does the organization provide to – (list stakeholders)

The following checklist called from the guidelines for the Ghana.gov portal can give an indication of information that should be provided as a very minimum by each MDA.

Web Site Content Checklist

- Table of Contents
- MDA Information
  - About this organization
  - Management/Key personnel
  - MDA background - mandate
  - Awards/Professional affiliations
  - Directions to office/Contact information
  - Job postings
  - Others
- Marketing and Sales Information
  - Calendar of upcoming events
  - Product description (text, pictures, videos)
  - Online catalog of available products and services
  - Customer testimonials or quotes
  - FAQs (frequently asked Questions) with answers
  - Press releases and contacts
- Customer Service Information

- Usage tips
- Product/services updates
- Training resources
- Support telephone numbers
- Common questions and answers
- Others

- Other Information

  - Links to related sites
  - Research findings
  - Resources (books, videos, contacts)
  - Others

Which services can be improved or would benefit from using/adopting web technologies

Having evaluated the web presence of the organization, it will be necessary to construct the web interface takings into account the standards identified by the E-GMO.

Consideration of services that would benefit from being web based can be evaluated under any of the following headings:

What information can we/should we publish – Can we use ICT to expand access to Government Information

Identify information that would be useful to various stakeholders if published.

How can we interact with our users and broaden civic participation in Government

Determine how to improve stakeholder involvement in government activity by providing users with the ability to interact with policy members right through the process of policy formulation. Interactive government involves two-way communication between government agencies and users of their services. This will solicit feedback, engage the users, and enable them to collaborate in driving the government's agenda.

How do we improve service delivery to users by making government services available online?

This will allow users to process transactions online. This will offer users a direct link to government services and provide additional service delivery channels. Examples will include filling in online application forms, submitting periodic returns, etc.

How can stakeholders gain extra value by interacting with government?

To Customers

Is the service already provided (manually)

Will online provision of the service enable customers initiate, track and conclude services at any time and from anywhere.

Will processing times associated with the service be significantly reduced by providing it online.

To Organisation

Will procedures within the agency be simplified as a result of the service being online?

Can the service be provided without substantial additional cost?

Can the service be automated?

Will staff be relieved of routine work?

Is the service very visible to the external stakeholders?

Will the image of the agency be enlarged by the provision of this service?

Organisational Complexity

Scope of the procedure

How many actions are involved in providing the service?

How much change is required to the internal workflow in order to be able to provide the service sensibly online?

Technical complexity / challenge / implementability

A service can only be rated “technically complex” if it ties up a lot of staff full-time (e.g. application for **legal** registration, repayment of student loan, etc.). In this case, most of the necessary technical equipment is also used only for that service.

In the case of services whose scope is smaller, this will generally not be the case. In these instances, the technical complexity can only be specified for a group of services or for a group of service elements (e.g. all service elements which require a qualified electronic signature, or all service elements that entail online payment). In these cases, there are a few questions that can be answered only for a set of services.

Technical Scope

Will a lot of workstations have to be equipped with new computers or other new IT equipment (printers, scanner etc.)

Will a lot of personal computers need to be reconfigured or provided with new software?

Does this service make high demands on other items of IT equipment (servers, routers etc.)

Necessity for electronic signatures and legally binding time stamps

Is it obligatory or desirable for documents to be signed by the agency?

Is it necessary to receive signatures (Does the customer need to be able to give a signature)

Is a legally binding time stamp necessary?

Necessity for encryption

Is it necessary to use or offer encrypted communications?

Introduction of special systems

Is it necessary to set up an electronic workflow (or to extensively change one) in order to achieve the above objectives regarding the online provision of service e.g. Customs GCNET?

Is it necessary to set up an automated processing system in order to achieve the above objectives regarding the online provision of service?

Can a standard solution be used or will there be a need for a unique bespoke development.

Introduction of a procedure for online payments

Is it necessary to collect fees online

Provision of time-critical services

Will it be necessary to specially protect the computer system against occasional failures?

Archiving, reproducibility, readability

For how long do documents associated with the service have to be archived or remain readable, i.e. how long do reading facilities and storage media need to be retained for.

How big is the technical effort and technical challenge?

Personnel

Experience with regard to implementation

Is there enough experience available in-house (especially as regards organization and IT) to plan and execute implementation of the service in-house

State of knowledge and qualification requirements regarding application

Do the staff have enough knowledge to implement the changes to the future daily routine that are necessary.

What is the likelihood of staff readily accepting the change?

Will implementation of the service meet with acceptance among the staff affected?

What is the likely cost?

Quantify the benefits that you expect the organization to derive.

Evaluate the costs against the benefits.

Technology

Is the necessary technology already available?

Money

Is any money available in the budget plan for implementation of this service.