Ethiopian National Enterprise Architecture Framework (ENEAF) and Ethiopian eGovernment Interoperability Framework (EeGIF) Revision Project

EXECUTIVE SUMMARY

MINISTRY OF INNOVATION & TECHNOLOGY | ADDIS ABABA, ETHIOPIA

SUBMITTD BY – SCHOOL OF INFORMATION SCIENCE, AAU

Executive Summary

Per the agreement made in between SIS-AAU and MInT, the consulting team has revised (developed an extension version of NEAF and EeGIF. The main purpose of the revision project is to generate an updated/extension of the existing NEAF and EeGIF documents with the aim of facilitating their implementation. Accordingly an attempt has been made to emphasis on governance structure, architectural principles, technical standards, implementation roadmap and updating facts explaining the current NEAF and EeGIF ecosystem.

Architecture framework can be defined as a collection of **c**onventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders. A framework is fundamentally a conceptual model and a structure within which the key components of the architecture and the relationships between these components are defined. As presented in one of our reports, a framework;

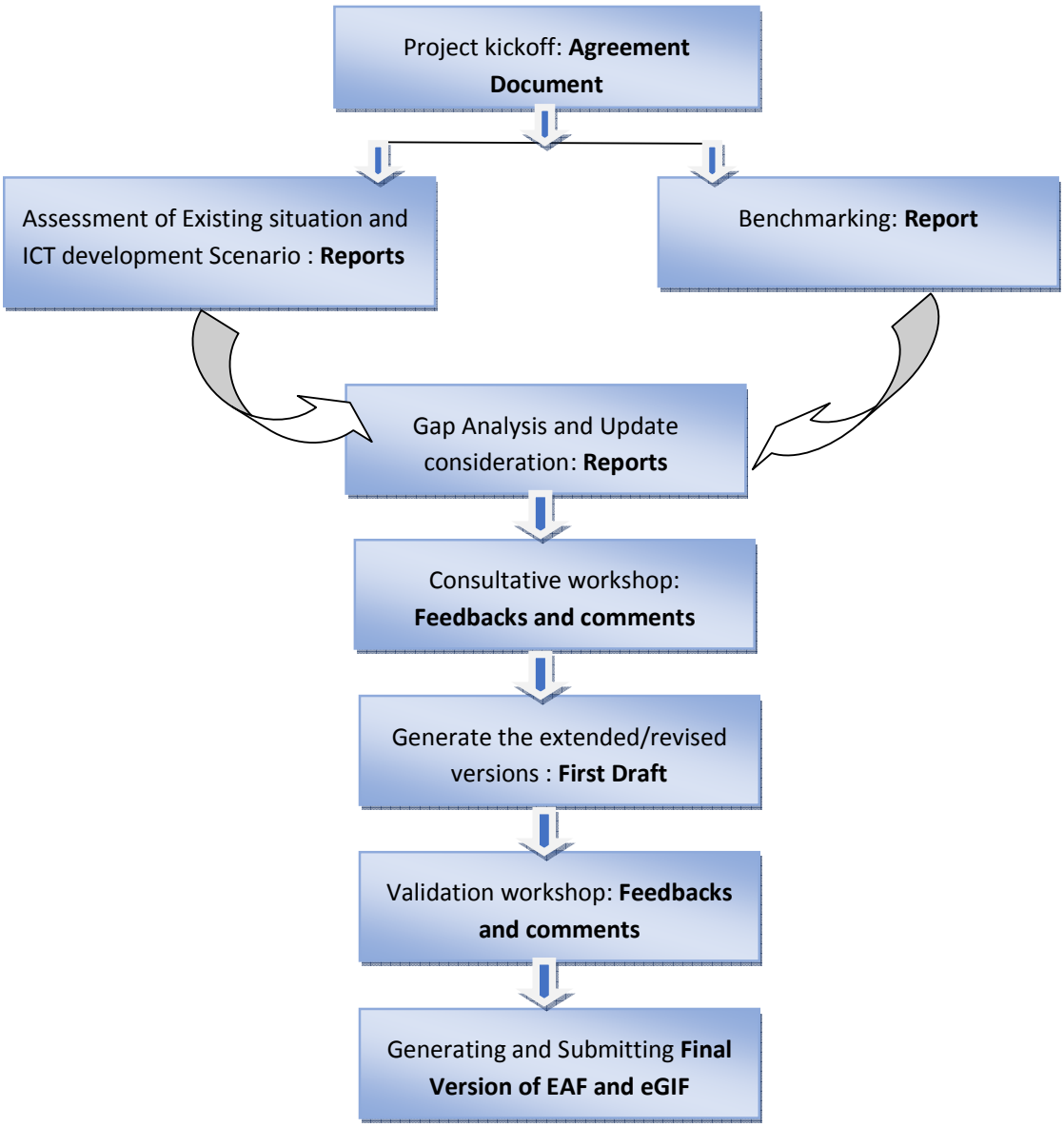
- Helps to organize thinking about the architecture
- Level-sets stakeholders about the contents of the architecture by providing common definitions and concepts. It helps to ensure that everyone is using the same set of semantics and presents them to the group of stakeholders interested in the contents of the architecture.
- Provides a description of the architectural artefacts
- Shows the relationships between business and technology elements, ensuring that there is coherence between all elements and that every business element can map to a corresponding element in the technical architecture and, similarly, that technical elements can be seen as supporting key business requirements.
- Provides a way to communicate the architecture

This executive summary document presents how NEAF and eGIF are prepared, visualized and presented as a package of document/reports comprising both frameworks.

Generally, both empirical and desk research approaches were used in the process of revising the existing EAF and eGIF. Accordingly the following four major tasks were done;

- Desk research: to understand theoretical underpinning
- Empirical data collection data analysis: to document the existing situation current ICT development scenario
- Benchmarking : to learn from forerunner in the area in terms of methodology use, representations and related matters
- Update/revise NEAF and eGIF documents
- Validation workshops: for collecting feedbacks and inputs as well as validating the documents

The diagram below is a pictorial representation for the whole process in revising the frameworks.



In the context of this document, Ethiopian National Enterprise Architecture Framework is visualized in terms of principles, governance and an implementation road map. The national EAF guides the development of architectural elements for the four core (Business, Application, Data and Technology) and four crosscutting elements (Security, Performance, Integration and Governance). eGIF on the other hand, is an element of NEAF facilitating Integration and thus it is represented with detailed principles, policies, standards, governance and roadmap.

In line with the revision objective and envisaged implementation of both frameworks the following table highlights major changes made on the previous documents

S.N	Major Sections of the Previous Document (NEAF V.5.0)	Remark regarding changes /revisions	Reference to the current version
Changes and additions made on NEAF			

1	Overview of the existing Enterprise Architecture Frameworks	Changes has been made by employing selection criteria's	Review of EA Frameworks and Update consideration (Gaps)*
2	Comparison of Frameworks	Changes made on the assessment of the selected Frameworks	Review of EA Frameworks and Update consideration (Gaps)*
3	Enterprise Architecture Frameworks Adopted by Countries	Changes made by diversifying selected countries for benchmarking	Benchmarking Report*
4	Selection of frameworks for Ethiopian Government	Changes made to reflect the current situation	Assessment of the ICT Development Scenario in Ethiopia*
5	Development of EA framework for Ethiopia	Changes made to extend and elaborate on governance, principles, implementation road map	**NEAF Governance and Compliance **** **NEAF Architectural principles **** **NEAF and eGIF Implementation Roadmap****

Changes and additions made on eGIF			
S.N	**Major Sections of the Previous Document (eGIF V.1.0)**	**Remark regarding changes /revisions**	**Reference to the current version**
1	Summary of As-Is Assessment	Changes made to reflect the existing situation	Report on Review of Existing Situation & Benchmarking in eGovernment Interoperability*
2	Learning from leading practices	Changes made by diversifying countries selected to complement	Report on Review of Existing Situation & Benchmarking in eGovernment Interoperability*[i]
3	Ethiopian e-Government Interoperability Framework (EeGIF)	Further refined in line with NEAF	**eGIF Governance and compliance ****
4	EeGIF Standards	Changes made to reflect current situation	**EAF and eGIF Technical Standards ****
5	EeGIF Governance Structure	Changes made to facilitate implementation	**eGIF Governance and compliance ****
6	Implementation Plan	Revised	**NEAF and eGIF Implementation Roadmap****

Finally, the following major deliverables (documents) are submitted as a package of both frameworks;

NEAF documents

- Ethiopian National Enterprise Architecture Framework – Extension Benchmarking
- Assessment of the ICT Development Scenario in Ethiopia
- Review of EA Frameworks and Update consideration (Gaps)
- **NEAF Architectural principles**
- **NEAF Governance and Compliance**
- **NEAF and eGIF Implementation Roadmap**

eGIF documents

- Report on Review of Existing Situation & Benchmarking in eGovernment Interoperability
- Report on Gap Analysis for E-eGIF Revision
- **NEAF and eGIF Technical Standards**
- **eGIF Governance and compliance**

As can be seen from the above details, the project has delivered the EAF in general and specific details for the governance and integration (through interoperability framework) aspects of the EAF. Accordingly we strongly recommend development of framework details for the remaining elements.

[i] *- already submitted reports
**- submitted along with this executive summary

Ethiopian National Enterprise Architecture Framework (ENEAF) - Extension

ENEAF GOVERNANCE& COMPLIANCE

MINISTRY OF INNOVATIONS & TECHNOLOGY | ADDIS ABABA, ETHIOPIA

Document Description

Document Title	Ethiopian National Enterprise Architecture Framework – Extension ENEAF Governance& Compliance
Document version	0.2
Document Status	**Draft**
Author(s)	Ermias Abebe WondwossenMulugeta (PhD) MesfinKifle (PhD) TibebeBeshah (PhD) WorkshetLamenew (PhD)
ENEAF Decision	Under Review

Version Control

Version	Date	Description of changes made
0.1	27/10/2019	Draft document
0.2	04/11/2019	Draft Document

Document Validation

Version	Authors	Reviewed by	Date	Status
0.1	ERMIAS ABEBE WONDWOSSENMULUGETA (PHD) MESFINKIFLE (PHD) TIBEBEBESHAH (PHD) WORKSHETLAMENEW (PHD)	-	27/10/2019	DRAFT
0.2	ERMIAS ABEBE WONDWOSSENMULUGETA (PHD) MESFINKIFLE (PHD) TIBEBEBESHAH (PHD) WORKSHETLAMENEW (PHD)		04/11/2019	DRAFT

List of Acronyms

CIO	Chief Information Officer
EA	Enterprise Architecture
EeGIF	Ethiopian Electronic Government Interoperability Framework
EAF	Enterprise Architecture Framework
ENEAF	Ethiopian National Enterprise Architecture Framework
FPI	Federal Public Institution
GIF	Government Interoperability Framework
ICT	Information and Communication Technology
IndEA	India Enterprise Architecture
IT	Information Technology
MinT	Ministry of Innovation and Technology
NEAF	National Enterprise Architecture Framework
NGEA	(Nigerian Government Enterprise Architecture)
NITDA	Nigerian Information Technology Development Agency
PMO	Prime Minister Office
SDG	Sustainability Development Goal
TWG	Technical Working Group

Contents

Executive Summary

"Governance" identifies the planning, decision-making, and oversight processes and groups that will determine how the EA is developed, verified, versioned, used, and sustained over time with respect to measures of completeness, consistency, coherence, and accuracy from the perspectives of all stakeholders.In line with this, development and implementation of EA requires envisioned governance that spans national, federal and regional structures. This document reflects the proposed governance arrangement of ENEAF.

The document contains the processes, organizational structure, roles and responsibilities and the associated elements of the proposed ENEAF governance. While the structure is designed to show both the ENEAF and EeGIFaltogether, the details of ENEAF are presented in the current document and that of the EeGIF are depicted in a separate document.

1 Background

In Ethiopia, the ministries and agencies are essential for the success, sustainability and institutionalization of the reform underway and have their respective and varied mandates. Recently, nation-wide emphasis is given to digital transformation to improve government services. The United Nations e-Government Survey 2016 emphasizes three things - a Whole-of-Government approach, Policy Integration and use of Big Data Analytics - as the important means of achieving theSustainable Development Goals (SDGs). Achieving the a Whole-of-Government and Government Digital Transformation requires among others a re-arrangement of the national enterprise architecture, IT governance systems, and procedures in the ministries and agencies. This calls for a placement of a National Enterprise Architecture framework (NEAF) Governance in the country.

“Governance” identifies the planning, decision-making, and oversight processes and groups that will determine how the EA is developed, verified, versioned, used, and sustained over time with respect to measures of completeness, consistency, coherence, and accuracy from the perspectives of all stakeholders.Governance is essentially about ensuring that business is conducted properly. It is less about control and strict adherence to rules, and more about guidance and effective and equitable usage of resources to ensure sustainability of an organization’s strategic NEAF objectives.

In connection with this, the notion Architecture Governance refers to the institutional mechanism, along with definedroles and responsibilities, for the development and maintenance of Enterprise Architectures within anorganization, besides the review of compliance.

National Enterprise Architecture Framework (NEAF) is an aggregation of models and metamodels, governance and compliance mechanisms, technology standards, and guidelines put together to guide effective development and implementation of EA by different government entities across the country.It provides a practice and orientation by which organizational architectures can be effectively managed and controlled at an enterprise level.

NEAF would help in envisioning the requirements of improved government services, managing complexity, managing IT portfolio, delivering a road map for changes, supporting system development, supporting business and IT budget prioritization, etc. Different issues in any organization like legacy transformation, business changes, infrastructure renewal, and application systems renewal and business/IT alignment can be resolved by designing an Enterprise Architecture (EA).

In view of this, ENEAF governance structure consisting of the enactment duties and responsibilities is proposed based on the assessments conducted earlier with the view to produce subsequently the EA reference models for ministries and agencies to use as a base for producing their respective architectures, for MinT to conduct the role of supervision to ensure other ministries and agencies comply to standards, policies and guidelines.

2 Purpose of this Document

Thepurpose of this document is to show the ENEAF Governance Structure. The recommended governance structure for ENEAF is a federated architecture governance model and it provides advantages in cost, schedule, autonomy, scalability, and robustness.

3 Governance Processes

The governance processes include: top-down processes and bottom-up processes. The top-down processes are activities or functions related to advisory and enforcement. The advisory and guidance services are supposed to be provided from the prime minister office digital transformation experts to the governing councils and the coordinating unit to be located at MinT as shown in figure 1 and figure 2 in the next section. The ministries, agencies and regional offices are supposed to be guided and advised by the coordinating unit, governance council and the prime minister office. While review processes are conducted by the prime minister office and the governing council, compliance checking processes are performed by the coordinating unit.

The bottom-up processes are initiated from the ministries, agencies and regional offices. These include: placing requests for advices and guidance, approval of project budgets, approval of organizational activities such as EA architecture development and setting standards specific to their organizations. The academic institutions, professional associations and development partners also involve in many ways in the process of conducting research, capacity building and consulting.

4 Proposed ENEAF Governance Organization Structure

4.1 ENEAF Ecosystem

The major stakeholders/members of the ENEAF ecosystem are depicted below in the diagram. Such stakeholders as the private firms and the citizens are not included as the scope of this current document is dealing with the parties that majorly involve in the development and implementation of the ENEAF.

Figure 1: Proposed ENEAF and EeGIFEcosystem

While the detailed roles and responsibilities of the stated members are shown in the governance structure in the next section, a high level of activities supposedly to be performed by the members shown in the previous figure are tabulated as follows.

Table 1: High Level Description of the Ecosystem Members

Ecosystem Members	**Activities**
The Prime Minster Office	Guidance and Approval, provides development vision resources
The Ministry of Finance	Approval, provides resources

Governing Council at MinT	Provides architecture vision Provides approvals and resources Reviews and manages Reports to the Prime Minister and Ministry of Finance
Central Coordinating Unit	Build, implements, manage, review Reports to the Governing Council, PM and Ministry of Finance
Government Ministries & Agencies	Request approvals (budget, projects, etc) Prepares EA and standards
Academic & Research Institutions	Provides training, research and consultancy
Professional Associations	Provides training, research and consultancy
Development Partners	Provides consultancy & financial assistance

4.2 Governance Organization Structure

The governance structure is built basically on three pillars. The prime minister office together with the Ministry of Finance are labeled as “the Sponsor” who provides development vision and resources. The governing council is labelled as “the Thinker” responsible for creating architecture and standards vision, review compliances and manages IT governance activities. The third pillar is the central coordinating unit responsible for building, implementing and managing architectural and standards related issues and labelled as “the Doer”.

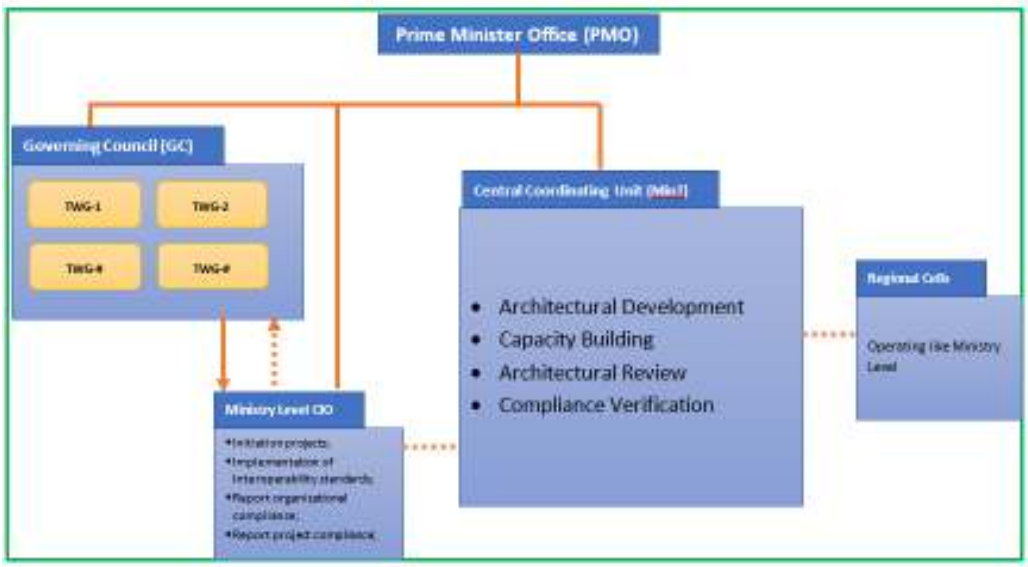


Figure 2: Proposed ENEAF and EeGIF Governance Structure

5 Governance Roles and Responsibilities

The roles and responsibilities of the entities defied in the governance structure including the membership constituencies are presented as follow.

A) Governing Council (GC)

The Governing council is the highest body for decision making of EA and eGIF related activities. The council is responsible for overseeing and supervising the entire process of cross-organizational e-Service delivery in line with the digital transformation plan. The Committee will work to ensure all standards are complied with.

Membership

- ✓ Headed by Delegate from the PMO
- ✓ State Minister of MInT will be the Secretary
- ✓ Members: State Ministers of
  - ➢ All Ministries Represented by their CIOs or equivalent
  - ➢ Attorney General
  - ➢ Three Private Sector Representatives
  - ➢ Donor Representatives
  - ➢ Representatives from Professional Associations
  - ➢ Representatives Higher Learning Institutions

Roles and Responsibilities:

1. Topics and decisions of the Council are to be prepared by the Secretary.
2. The council should approve all strategic initiatives in the field of IT developments of the ministry:
   - ✓ take decisions and responsibility of reengineering processes needed for the implementation of new projects.
   - ✓ Meet annually to assess the compliance level of stakeholders with the provision of the framework.
   - ✓ Coordinate (where necessary) or assist in the development, promotion and adoption of standards, guidelines and policies that will help ensure the actualization of the purpose of this framework.
   - ✓ Coordinate the review and update of the framework in line with the provision the EeGIF.

- ✓ Envision and serve as decision-making arm the execution arm
- ✓ provides guidance and assistance to the government ministries and agencies and enable them to enhance EA maturity
- ✓ guides the development of EA reference models, repository and detailed standards at national, federal and regional levels identified in the roadmap
- ✓ Reviews and approves documents generated by the chief architect
- ✓ Meet annually to assess the compliance level of stakeholders with the provision of the ENEAF.
- ✓

B) Technical Working Group (TWG)

Various Technical Working Group shall be formed by and from the members of the Governing Council who will be responsible for formulation, revision, monitoring and actual implementation of the EeGIF and report to the GC as and when required.

C) Central Coordination Unit (MInT)

The Central Coordination Unit is the responsible unit under MInT who will be tasked with the responsibilities of devising, enacting, drafting, enforcement and monitoring of the eGIF. The central coordinating Unit will mainly be responsible for:

a. Architectural Development
b. Architectural Review
c. Capacity Building
d. Compliance Verification

Roles and Responsibilities:

1. Responsible for ICT strategy planning, implementation and supervision processes. Dealing with public relations on information society issues.
2. Has a right to get information from government bodies about the use of ICT systems and about the results of systems development processes.
3. Responsible for drafting the ICT budget in the state budget in cooperation with the Ministry of Finance. The Unit supervises the most important development projects which might also look into the compliance to EeGIF;
4. Responsible for coordination of drafting of the main ICT-related legal acts (Digital Signature Act, Personal Data Protection Act, Telecommunications Act, Databases Act, etc.) The Unit should have a right to present opinions and approve all ICT-related legal acts which could be initiated by the appropriate ministry;
5. Monitors the compliance of the reference models and standards

6. Checks interoperability across platforms and services
7. Ensures cost effective implementation of EeGIF and standards
8. Ensures consistent integration among ministries and agencies
9. Ensures improved and optimized resource utilization
10. Has the right to initiate new ICT-related legal acts
11. Responsible for management of the work of CIO working groups, planning and implementing CIO training activities.
12. Coordinates international cooperation activities in the field of ICT. Often international cooperation is performed in other ministries (e-health issues – Ministry of Health, basic ICT infrastructure issues – Ministry of Innovation and Technology, etc.) but the central coordination should be performed by the Central Coordination Unit.
13. Initiates cross-government projects and programs.
14. Responsible for general guidance, recommendations and standards.
15. Prepares EA and standards learning packages
16. Organize training for stakeholders
17. Create links with Vendors, Academic institutions and IT professional associations for preparation of trainings, learning materials, and organize certifications

D) Ministry Level Chief Information Officer (CIO)

The Central Coordination Unit needs to have contact points in ministries to cooperate with them. CIOs should be nominated at the ministry level (normally he/she should be at the level of a Head of Department or an advisor to the ministry) with the following responsibilities:

Roles and Responsibilities:

1. Create and implement ICT action plan at the ministry level.
2. Plan and prepare for approval the annual ICT budget for the ICT Council of the ministry. The ICT budget should be in line with both the government ICT action plan and the ministerial action plan.
3. Implement different projects related to procurement, supervision of projects, ICT training issues of ministries, etc.
4. Organize ICT systems maintenance and user help desk.
5. Organize end user training on ICT issues.

6. The CIO should be a member of the ICT workgroup of CIOs of ministries led by the Central Coordination Unit.

E) Regional Cells

The Regional Cells, based on the federal structure of the Ethiopia, will act like Ministry level CIOs and collaborate with the Central Coordinating Unit (MinT) for capacity building and compliance.

6 Governance Checkpoints and Success/Failure Criteria

The following items if enacted are key to the successful accomplishment of ENEAF and EeGIF.

1. The previously depicted governance structure is of generic. While re-organization of the structure and definition of the roles and responsibilities can be further looked contextually at the PM, MinT and the rest of the ministries and agencies, certain important roles if considered carefully would make the exercise of developing EA and ensuring compliance is of paramount importance. These include the involvement of Chief Enterprise Architect, Enterprise Business Architect, Enterprise Application Architect, Enterprise Data Architect, Enterprise Technology Architect and Enterprise Security Architect.
2. Communication is at the canter of all success and effectiveness of EA and GIF undertakings. Communication plan that lays down the processes relating to Why, How, When, and With Whom communication need to take place. For any enterprise architecture communication to be effective, it must be integrated with its core processes and structure. To achieve this, a robust architecture communication framework is required. Among others building awareness, entertaining feed-back mechanisms, creating shared understanding among the ecosystem members, facilitation and coordination that involve clear and genuine flow of information, regular preparation and submission of reports that involve immediate or quick exchange of comments and suggestions to enhance the level of EA and standards maturity are crucial for the success and effectiveness of the EA and GIF undertakings.
3. Such communication tools as creating portals that help to manage knowledge of the members of the ecosystem and bring them to exchange knowledge by uploading and downloading documents, organizing EA and GIF repositories to store EA principles, reference models, guidelines, standards and policies are crucial for the success of the EA and GIF

undertakings. What's more conducting various trainings in various ways, reviewing and updating EA and GIF repositories, using emails, preparing videos, organizing seminars, workshops and conferences that present case studies contribute to the success of the EA and GIF undertakings.

4. Strategic control of giant IT projects through Public-Private partnership (PPP) should be given emphasis of these projects to show enduring and sustainable results.
5. Enforcing the EA and GIF compliance through various means such as EA and GIF maturity assessment has great contribution to the maintenance of EA and GIF activities which would ensure success in all endeavours.

Ethiopian National Enterprise Architecture Framework (ENEAF) - Extension

ARCHITECTURAL PRINCIPLES

MINISTRY OF INNOVATIONS & TECHNOLOGY | ADDIS ABABA, ETHIOPIA

SUBMITTED BY : SCHOOL OF INFORMATION SCIENCE, AAU

Document Description

Document Title	Ethiopian National Enterprise Architecture Framework – Extension **Principles**
Document version	0.2
Document Status	**Draft**
Author(s)	Ermias Abebe WorkshetLamenew (PhD) Wondwosen Mulugeta (PhD) Mesfine Kifle (PhD) Tibebe Beshah (PhD)
ENEAF Decision	Under Review

Version Control

Version	Date	Description of changes made
0.1	20/10/2019	Draft document
0.2	03/10/2019	Draft document

Document Validation

Version	Authors	Reviewed by	Date	Status
0.1	ERMIAS ABEBE WORKSHETLAMENEW (PHD)	-	20/10/2019	DRAFT
0.2	ERMIAS ABEBE WORKSHETLAMENEW (PHD)	-	03/10/2019	

1 List of Acronyms

BPR	Business Process Reengineering
DB	Doing Business
EA	Enterprise Architecture
ENEAF	Ethiopian National Enterprise Architecture Framework
FDR	Federal Democratic Republic [of Ethiopia]
ICT	Information and Communication Technology
KPI	Key Performance Indicators
MDA	Ministry, Department, Agency, Authority
PRM	Performance Reference Model
RFP	Request for Proposal
SDG	Sustainable Development Goal
TOGAF	The Open Group Architecture Framework
UN	United Nations
US FEAF	(United States Government) Federal Enterprise Architecture Framework

Contents

2 Executive Summary

The definition of architecture principle is fundamental to the development of any enterprise architecture.The Ethiopian National Enterprise Architecture Framework (ENEAF) recommends a set of principles in different domains tobe adopted at the national level.

Architecture Principles should be aligned with not only business principles but also with business goals and drivers defined by the Government to consolidate at the national level as reference to be used for individual Enterprise Architecture within MDAs. ENEAF ensures that the definitions of those business principles, goals and strategic business drivers are current and unambiguous.

The ENEAF is, thus, developedfrom a set of business principleswhich are derived mainly from the constitution of the FDR of Ethiopia, the GTP 2, the UN-SDG, the “ease of doing business” and “home-grown economic reform” strategies developed by the Prime Minister’s office. The principles are also aligned with relevant policies as well as other legal or regulatory compliance needswithin the nation.

Domain specific Architecture gets influenced by relevant architecture principles and hence it becomescritical task for the EA Governance Body to approve the architecture principles proposed by any MDA.

3 Introduction

Enterprise Architecture Principles are high level statements of the fundamental values that guide business informationmanagement, information technology (IT) decision-making and activities, and are the foundation for both business and IT architectures, standards, and policy development. These principles are general rules and guidelines that may be subject to adjustments as the enterprise refocuses its objectives and mission. However, theyare intended to be enduring and not prone tofrequent amendments.

Principles represent the highest level of guidance for IT planning and decision making. Principles are simple statements of an organization's beliefs about how it wants to deploy IT services over the long term and are derived from business goals and vision.A good set of principles will be founded in the beliefs and values of the organization and expressed inlanguage that the business understands and uses. Principles should be future-oriented, endorsed andchampioned by senior management. They provide organization foundation for making architecture andplanning decisions, framing policies, procedures, and standards, and supporting resolution of contradictorysituations.

Architecture principles are chosen to ensure alignment of IT strategies with business strategies and visions.Specifically, the development of architecture principles is typically influenced by the following:

- **Government and sector mission and plans:** The mission, plans, and organizational infrastructure of the enterprise.
- **Government strategic initiatives:** The characteristics of the enterprise — its strengths, weaknesses,opportunities, and threats — and its current enterprise-wide initiatives (such as process improvementand quality management).
- **External constraints:**citizen expectations, existingand potential legislation, etc.
- **Current systems and technology**: The set of information resources deployed within the enterprise,including systems documentation, equipment inventories, network configuration diagrams, policies,and procedures.
- **Computer industry trends:** Predictions about the usage, availability, and cost of computer and communicate on technologies, referenced from credible sources along with associated best practices presently in use.

Decisions and business cases are strengthened by compliance with these principles. Where there are conflicts of interest between, for example, two solution development projects, then these principles should guide the decision making. If proposed changes do not comply with these principles,then the changes should be realigned with the principles.

The following five criteria distinguish a good set of principles:

- **Understandable:** the underlying tenets can be quickly grasped and understood by individualsthroughout the organization. The intention of the principle is clear and unambiguous, so that violations,whether intentional or not, are minimized.
- **Robust:** Enable good quality decisions about architectures and plans to be made, and enforceablepolicies and standards to be created. Each principle should be sufficiently definitive and precise tosupport consistent decision-making in complex, potentially controversial situations.

- **Complete:** Every potentially important principle governing the management of information andtechnology for the organization is defined. The principles cover every situation perceived.
- **Consistent:** Strict adherence to one principle may require a loose interpretation of another principle.The set of principles must be expressed in a way that allows a balance of interpretations. Principlesshould not be contradictory to the point where adhering to one principle would violate the spirit ofanother. Every word in a principle statement should be carefully chosen to allow consistent yet flexibleinterpretation.
- **Stable:** Principles should be enduring, yet able to accommodate changes. An amendment processshould be established for adding, removing, or altering principles after they are ratified initially

4 Document Objectives

This document describes architectural principles for ENEAF. Principles are established on all enterprise architecture domains:

- **Business**- provide a basis for decision--making throughout the business
- **Data**- provide guidance of data use within the enterprise
- **Application**- provide guidance on the use and deployment of all IT applications
- **Technology**- provide guidance on the use and deployment of all IT technologies

Four more sets of principles are identified which work across the four major architecture domains. These are:

- **Performance –** provide a basis for monitoring and evaluating effectiveness and efficiency**.**
- **Governance –**provide basis for measurement, management, and steering processes for a business domain or information systems that provides the expected level of result.
- **Security -**providethe basis for developing and enforcing securitystandards, policies, and norms to be developed and followed, since it is an enforcement point for InformationTechnology.
- **Integration –**provide the basis for bringing the other perspectives together in order to provide a seamless citizen experience at all levels.

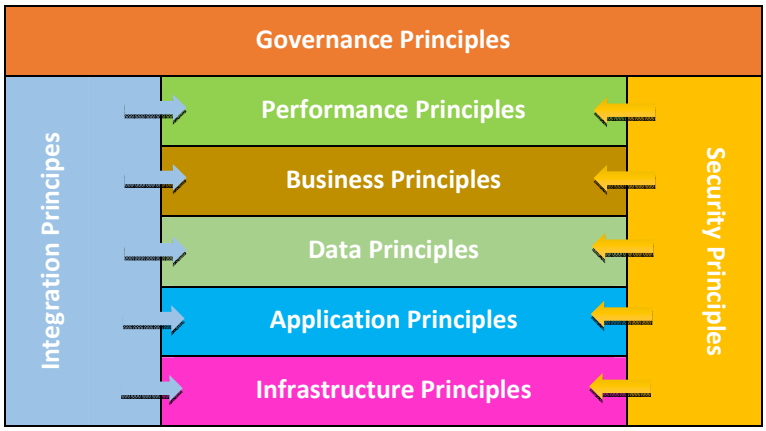


Figure 1: Consolidated principles

EA guiding principles are important for defining criteria by whichtechnology andservices, that span or impact the enterprise, are managed, acquired, designed and configured. Each principleincludes several statements that describe general traits, outcomes we want to achieve, and useful constraints. The guiding principles should:

- be included in RFP's and procurement processes;
- guide decision-making;
- be used to evaluate services, products, and projects; and
- inform system design and development

5 Scope and Application

5.1 Scope

The scope of these principles includes services that are delivered entirely within the boundaries of the government of the FDR of Ethiopia.

MDAs should be able to map these principles to their ICT vision and strategic plans, as well as to whole-of-government strategic guidance. MDAs should adapt the principles to meet their specific business needs, through mapping of specific actions (such as EA development, business initiatives, ICT acquisitions and implementation) to the principles. The principles relate to the delivery of business services undertaken by the Government and should not be seen as being constrained to the delivery of ICT related services.

5.2 Application

Architecture principles are used to capture the fundamental truths about how the Government will use anddeploy IT resources and assets. Ministries, Departments (including all the various forms of government unit such as Centres, Commissions, Offices, etc excepting Agencies and Authorities)., and Agencies and Authorities (MDAs) can use the principles in several ways:

- To provide a framework within which the Government can start to make explicit, evidence-based decisions about IT
- As a guide to establishing relevant evaluation criteria, thus exerting strong influence on the selection ofproducts or product architectures in the later stages of managing compliance to the IT architecture
- As drivers for defining the functional requirements of the architecture
- To providea basis for justifying architecture activitiesusing the rationale descriptions
- To provide an outline of the key tasks, resources, and potential costs to the enterprise of following the principle using implication descriptions
- To provide inputs to assess both existing systems and the future strategic portfolio, for compliance with the defined architectures — such assessments provide valuable insights into the transition activities needed to implement an architecture in support of business goals and priorities
- To provide valuable inputs to future transition initiative and planning activities
- To support the architecture governance activities in terms of:
    - providing a “back-stop” for the standard architecture compliance assessments where some interpretation is allowed or required, and
    - supporting the decision to initiate a waiver request where the implications of a particular architecture amendment cannot be resolved within local operating procedure.

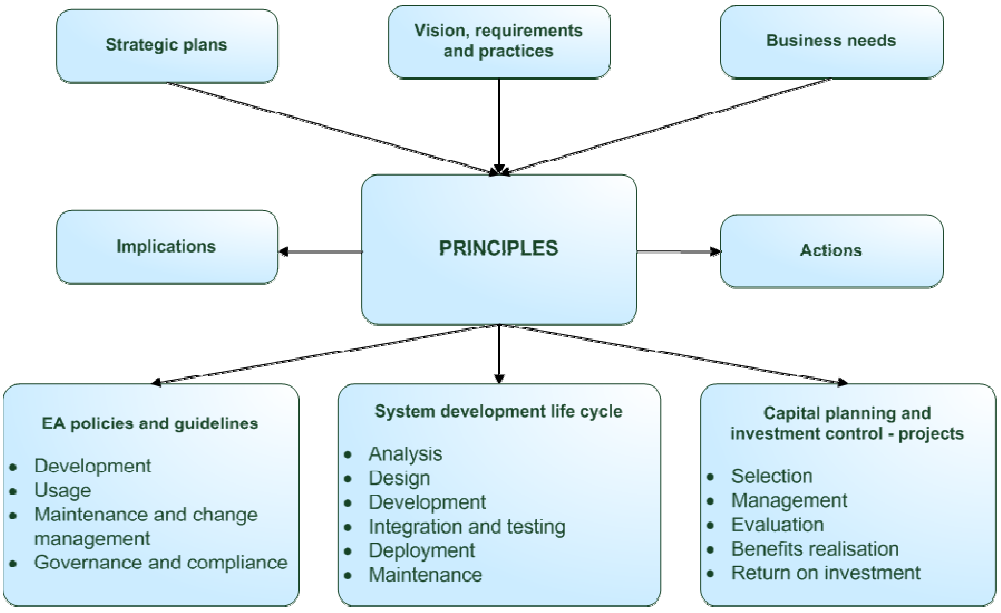


Figure 2: Role of Architecture Principles

6 Document Audience

ENEAF project stakeholders (business sponsors, architects, project managers, as well as functional and technical personnel) who are involved in specifying the EA scope and goals are the primary audience.

These principles apply toMDAs of the FDR of Ethiopia.MDAs should apply the principles as the basis for architectural planning and decisions across business environments.

7 Components of Architectural Principles

Architecture principles define rules and guidelines for the use and deployment of all IT resources and assetsacross the Government. They reflect a level of harmony among the various elements of the enterprise and helpin making future IT decisions. Each architecture principle should be clearly related back to the businessobjectives and key architecture drivers.

This document adopts the TOGAF approach to defining principles, as described in Table 1.The reasoning behind this is to promote understanding and acceptance of the principles and to support the use of the principles in explaining and justifying why specific decisions occur.

Accordingly, each of the principles are presented in full detail with the name of the principles, a short description, the rationale for the principle, and the implications of adopting the principle. The principles are numbered as PR-AA-X; the first two alphabets stand for “Principle”; the next two alphabets stand for the category of the alphabet; and the last digit is a serial number within the category.

Name	Should both represent the essence of the rule as well as be easy to remember. Specific technology platforms should not be mentioned in the name or statement of a principle. Avoid ambiguous words in the Name and in the Statement such as: "support", "open", "consider", and for lack of good measure the word "avoid", itself, be careful with "manage(ment)", and look for unnecessary adjectives and adverbs (fluff).
Statement	Should succinctly and unambiguously communicate the fundamental rule. For the most part, the principles statements for managing information are similar from one organization to the next. It is vital that the principles statement is unambiguous.
Rationale	Should highlight the business benefits of adhering to the principle, using business terminology. Point to the similarity of information and technology principles to the principles governing business operations. Also describe the relationship to other principles, and the intentions regarding a balanced interpretation. Describe situations where one principle would be given precedence or carry more weight than another for making a decision.
Implications	Should highlight the requirements, both for the business and IT, for carrying out the principle — in terms of resources, costs, and activities/tasks. It will often be apparent that current systems, standards, or practices would be incongruent with the principle upon adoption. The impact to the business and consequences of adopting a principle should be clearly stated. The reader should readily discern the answer to: "How does this affect me?". It is important not to oversimplify, trivialize, or judge the merit of the impact. Some of the implications will be identified as potential impacts only, and may be speculative rather than fully analysed.

Table 1: TOGAF recommended format for defining architectural principles

8 Overview of Architectural Principles

Table 2 below presents the summary of the principles presented in the following sections.

Principle (PR)	Short description
Performance (PP)	
PR-PP-1:Sustainability and ease of doing business linkage	Performance measurement systems derive from and are linked to SDGs and ease of DB goals prioritized by Government.
PR-PP-2: Outcome oriented	All Performance Measurement Systems are outcome-oriented.
Governance (GP)	
PR-GP-1: Primacy of Principles	These architectural principles will apply to all units within the Government.
PR-GP-2: Compliance with all statutory obligations	Enterprise data and information management processes comply with all relevant internal and external laws, policies, and regulations.
PR-GP-3: Transparency	The architectural decisions taken are transparent to all stakeholders.
Business (BP)	
PR-BP-1: Unity in Diversity	EA decisions are made taking full account of the needs of the citizen while at the same time addressing the wider goals of diversity and inclusion.
PR-BP-2: Maximise benefits to the Government	Information management decisions are made to provide maximum benefit to the Government.
PR-BP-3: Prioritisation of sustainability and ease of doing business initiatives	Enterprise Architecture efforts focus on the SDG and ease of doing business initiatives prioritized by the Government.
PR-BP-4: Business process re-engineering	Existing processes are re-engineered to eliminate non-value-adds and to make the services citizen-centric / business-centric.
PR-BP-5: Business continuity	All government services and business activities across the extended enterprise (ministries/agencies) should be operational in spite of systems failures and interruptions.
Application (AP)	
PR-AP-1: Sharing and reusability	All commonly used Applications are abstracted to be built once and deployed across the Government through reuse and sharing.
PR-AP-2: Technology and independence	Application Design is open standards-based and technology-independent.
PR-AP-3: Ease of use	Applications are easy to use, with the underlying technologies being transparent to the users.
Data (DP)	
PR-DP-1: Data is a national Asset	Data is a national asset that has specific and measurable value to the FDR of Ethiopia and therefore should be managed accordingly.
PR-DP-2: Data is shared	Data is shared across the MDAs to prevent creation and maintenance of duplicative sets of data by different agencies and ensure data access to users.
PR-DP-3: Data has trustee	Each dataset has a trustee accountable for data quality and security.
PR-DP-4: Common vocabulary and data/meta-data definitions	Data is defined consistently throughout all levels of Government, and the definitions are understandable and available to all users.
Technology (TP)	
PR-TP-1: Manage technical diversity	Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing

	environments.
PR-TP-2: Adopt standards and best practices	Designing and defining business processes, information systems, technology products and services used by ministries/agencies should adhere to industry standards and open architectures.
PR-TP-3: Future Proof	Enterprise Architectures are suitably designed and developed so as to be future-proof, not requiring frequent revisions with the advent of every new technology.
PR-TP-4: Shared infrastructure	IT Infrastructure is shared to ensure optimal utilization and effective maintenance.
Security (SP)	
PR-SP-1: Security by design	Security must be built into all stages and all aspects of architecture development.
PR-SP-2: High availability and disaster recovery	Technology architecture component and services should be deployed and configured in high available mode to provide maximum availability to business services.
Integration (IP)	
PR-IP-1: Interoperability	Interoperability is assured through adoption of open standards and open interfaces.
PR-IP-2: Openness and transparency	Government data is made open, barring exceptions, so that external parties can build services.
PR-IP-3: Primacy of user experience	All service interactions are designed with citizens at the core, by providing integrated multi-channel service delivery
PR-IP-4: Integrated multi-channel services	Integrated Services that cut across agency-silos are identified, designed and delivered through multiple delivery channels.

Table 2: Summary of ENEAF architecture principles

9 Principles in Detail

9.1 Performance Principles

PR-PP-1Sustainability and ease of doing business linkage	
Statement	Performance measurement systems derive from and are linked to SDGs and ease of DB goals prioritized by Government.
Rational	The government is working towards meeting the SDGs and Ease of Doing Business initiative.ENEAF and EAs at different levels should contribute towards the overall development of the nation.
Implications	• The Government defines its goals and objectives, which may be derived from and are linked to the sustainability development and ease of doing business goals. • The KPIs in the PRM must have parameters to measure the extent to which the Goals and Objectives are achieved.

PR-PP-2 Outcome oriented.	
Statement	All Performance Measurement Systems are outcome-oriented.
Rational	The overall objective of the Government is to deliver Services efficiently and effectively to the Stakeholders. The impact of these services on the stakeholders is measured via the effectiveness i.e. Outcome of the Services.
Implications	• This principle ensures that all development efforts should be measured by their outcome. • Investments are only made to achieve a certain outcome.

9.2 Governance Principles

PR-GP-1 Primacy of principles.	
Statement	These architectural principles will apply to all units within the Government.
Rational	The only way the government will be able to provide a consistent and measurable level of appropriately robust, reliable, sustainable services and quality information to decision makers, is if all stakeholders abide by these

	overarching principles for its business, data, application, and technology principles.
Implications	• This fundamental principle will ensure inclusion, consistency, fairness and continual alignment to the business. Without this the management of our technologies, information and business processes would be quickly undermined. • Business Partners engaging with the business will work to find accommodation between interested parties around any conflicts with a principle relevant to the proposal. • Information management initiatives will not begin until they are examined for compliance with the principles. • A conflict with a principle will be resolved by changing the framework of the initiative.

PR-GP-2 Compliance with all statutory obligations	
Statement	Enterprise data and information management processes comply with all relevant internal and external laws, policies, and regulations.
Rational	Enterprise policy is to abide by laws, policies, and regulations. This will not precludebusiness process improvements that lead to changes in policies and regulations.
Implications	• The enterprise must be mindful to comply with all laws, regulations, and external policies regarding the collection, retention, and management of data. • Continual education, access and awareness to the rules must be maintained. • Efficiency, need, and common sense are not the only drivers. Changes in the law and changes in regulations may drive changes in our processes or applications

PR-GP-3Transparency	
Statement	The architectural decisions taken are transparent to all stakeholders.
Rational	This principle is premised on the need for an open, honest, frequent and bidirectional communication between all stakeholders. EA is also expected to generate trust and reliability between all stakeholders.
Implications	• Will have buy-in from all business and IT stakeholders in the extended

	enterprise • There will be a need to develop a communication plan that must be followed across the extended enterprise • Will encourage open review forums for feedback in the EA process.

9.3 Business Principles

PR-BP-1Unity in diversity	
Statement	EA decisions are made taking full account of the needs of the citizen while at the same time addressing the wider goals of diversity and inclusion.
Rational	This principle representsthe essence of the “national” enterprise architecture framework. Ethiopia is a federal state which recognizes to the diversity of its constituents. This diversity could be expressed at all levels of the architecture.
Implications	• Enables the development and implementation of Enterprise Architectures independently and in parallel by all federal MDAs and federal states. • All development efforts should address diversity (multilingualism, legal context, capacity and capability differences, etc) at all levels of the architecture.

PR-BP-2 Maximise benefits to the Government	
Statement	Information management decisions are made to provide maximum benefit to the Government.
Rational	This principle embodies "Service above self." Decisions made from a Service-wideperspective have greater long-term value than decisions made from any particularMDA’s perspective. Maximum return on investment requires informationmanagement decisions to adhere to Service-wide drivers and priorities.
Implications	• Achieving maximum Service-wide benefit will require changes in the way theorganisation plans and manages information. Technology alone will not bringabout this change. • Some MDAs may have to concede their own preferences for the greaterbenefit of the entire government; • Application development priorities must be established by the entire government for theentire government;

	• Applications components should be shared across organisational boundaries;

PR-BP-3Prioritisation of sustainability and ease of doing business initiatives.	
Statement	Enterprise Architecture efforts focus on the SDG and Ease of Doing Business Initiatives prioritized by the Government.
Rational	Prioritization of Goals is an inevitable consequence of scarce resources competing to meet the huge expectations of the stakeholders of Government. There are two sources of such goals – the Sustainable Development Goals identified and articulated by the UN, and the Ease of Doing Business Goals promoted by the UN and endorsed by the Ethiopian government.
Implications	• Development projects at MDA level should prioritise sustainability and ease of doing business initiatives. • Budget clearance process should give priority to those projects that address SDG and Ease of DB goals.

PR-BP-4Business process re-engineering.	
Statement	Existing processes are re-engineered to eliminate non-value-adds and to make the services citizen-centric / business-centric.
Rational	New levels of performance in terms of better efficiencies, effectiveness and economy can't be achieved adopting the legacy systems and processes. A fundamental rethinking and redesigning is called for at the operational levels.
Implications	• Replacing legacy systems with systems that are compliant with the EA principles is encouraged. • New system development efforts should give priority to BPRed processes.

PR-BP-5Business continuity.	
Statement	All government services and business activities across the extended enterprise (ministries/agencies) should be operational in spite of systems failures and interruptions.

Rational	• Service design, implementation and deployment should ensure reliability of service delivery. • Government premises are able to continue the services regardless of external factors such as hardwarefailure and data corruption • Contingency plan should be devised to deliver the services on alternative mediums.
Implications	• Risk of business interruption will need to be established as dependency on shared systems is high • Risk management and mitigation plan will need to be developed across the extended enterprise. • These plans will not be limited to periodic reviews but will also include testing for vulnerability. • Mission - critical services should be identified and business continuity should be ensured through redundant and alternative capabilities. • Service design will address issues like recoverability, redundancy, and maintainability. • Level of continuity will need to be defined along with its recovery plan based on criticality and impact ofbusiness service.

9.4 Application Principles

PR-AP-1 Sharing and reusability.	
Statement	All commonly used Applications are abstracted to be built once and deployed across the Government through reuse and sharing. Sharing and reusability shall be subject to conformance with the principles of security & privacy.
Rational	Less duplicative capabilities will save lot of effort and cost for the ministries/agencies of the FDR of Ethiopia.
Implications	• Applications built across the Government will help not only particular ministry as we all complete Enterprise and it will lead to Enterprise wise resource utilization • Information system catalogue (inventory) shall be developed and used to identify candidates for common and transversal type applications. • Provision is made for Ministries/Agencies to (1) dispose or modify some of their unique applications in favour of a common/transversal application standard, and (2) adapt existing business processes to align with the common/transversal business process. • Common/transversal applications use open interfaces to enable development of departmental specific extensions and to enable

	information exchange with departmental unique application portfolio. • Ministries/Agencies retain data ownership to comply with legal or security requirements.

PR-AP-2 Technology independence.	
Statement	Application Design is open standards-based and technology-independent.
Rational	• Choice for different technologies will provide application's ability to run on multiple hardware and platforms. • Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way. • This will enable the Government to choose different technology platforms otherwise technology which is nearing obsolescence and vendor dependence become the drive rather than the user requirement themselves.
Implications	• It will provide portability of application and thus technology and platform-dependent. • It will enable legacy applications to interoperate with applications and operating environments developed under the enterprise architecture for the Government. • Middleware should be used to decouple applications from specific software solutions. • Application Software that does not support portability or platform independence is avoided. • Commercial Off the Shelf applications that are technology dependent are avoided. • Applications are designed for multi-tier deployment, which separates at least the end-user tier from the back-end tier, and the back-end tier from the database tier. • Traditional client-server applications that demands high-speed communications networks, high-performance end-user computers, or dedicated client (end-user computer) software, are not deployed over wide area networks.

PR-AP-3 Ease of use.	
Statement	Applications are easy to use, with the underlying technologies being transparent to the users.

Rational	• Simplicity of underlying technology will increase productive of user. Compromising user friendliness will lead to less productivity • Ease-of-use is a positive incentive for use of applications for the Government • It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the enterprise's integrated information environment • Training is kept to a minimum, and the risk of using a system improperly is low.
Implications	• Applications will have a common look and feel. • The common look and feel standard must be designed and usability test criteria must be developed. • Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. • User interface design is informed • by user location, language, competency, and physical capability. • Applications contain no unnecessary technical options that could reduce productivity and increase the risk of improper use of the application. • Same type applications have a common ‘‘look-and-feel’’, support ergonomic requirements and provide context sensitive help. • User friendliness is part of the test and acceptance criteria, which requires sign-off by an end-user representative, before applications are deployed for general use.

9.5 Data Principles

PR-DP-1 Data is a national asset.	
Statement	Data is a national asset that has specific and measurable value to the FDR of Ethiopiaand therefore should bemanaged accordingly.
Rational	• Data is a valuable resource; it has real, measurable value. Accurate and timely data is critical to quality ofservice. • A well-informed stakeholder and accurate information are critical to effective decision making, improvedperformance, and accurate reporting. It has no value when it remains in isolated pockets and hencemust be shared without compromising the security and confidentiality. • Data must be carefully managed and protected to ensure the data

	accuracy, accessibility andavailability for citizen and stakeholders.

Implications	• It will improve the information sharing/distribution environment to better disseminate information to thepublic and ministries/agencies of the FDR of Ethiopia.
	• The Government will identify authoritative sources for information, and agencies to provide access to specifieddata and information.
	• It will provide for the archival and preservation of all information (both in raw and aggregated form) exchanged, especially outside the government ecosystem, for future reference and if needed, for resolution of disputes. The Archival and preservation must be in accordance with the applicable regulatory requirements.
	• It shall force governmental units to make the cultural transition from ‘‘data ownership’’ thinking to ‘‘data stewardship’’ thinking.
	• Governmental units should ensure that data stewards have the authority and means to manage the data for which they are accountable.
	  ○ Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing the data must be assigned at the enterprise level.
	  ○ Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information.
	  ○ Data quality should be measured, and steps taken to improve data quality - it is probable that policy and procedures will need to be developed for this as well.
	  ○ A forum with comprehensive enterprise-wide representation should decide on process changes suggested by the data steward.

PR-DP-2 Data is shared.	
Statement	Data is shared across the Government Ministries/agencies to prevent creation and maintenance of duplicative sets of data by different agencies and ensure data access to users. Data Sharing shall be subject to conformance with the principles of Security & Privacy.
Rational	• Timely access to accurate data is essential to improve the quality and efficiency of enterprise decisionmaking at the national level as well as the organization level. • It is less costly to maintain and accurate data in a single repository than it is to maintain duplicative datain multiple repositories.

Implications	• To enable data sharing, we must develop and abide by a common set of policies, procedures, andstandards governing data management. • Data made available for sharing will have to be relied upon (timely and accurate) by all users to execute their respectivetasks. • Data sharing policy must be defined as part of Metadata Architecture. • Access to data does not necessarily grant the user access rights to modify or disclose the data. • Accessibility involved the ease with which users obtain information. • The way the information is accessed and displayed must be sufficiently adaptable to meet a widerange of user's and their corresponding methods to access.

PR-DP-3 Data has trustee.	
Statement	Each dataset has a trustee accountable for data quality and security.
Rational	• As the degree of data sharing grows and businessunits rely upon common information, it becomes essential that only the data trustee make decisions about the content of data. • Since data can lose its integrity when it is enteredmultiple times, the data trustee will have sole responsibility for data entry which eliminatesredundant human effort and data storage resources.
Implications	• Real trusteeship dissolves the data "ownership" issues and allows the data to beavailable to meet all users' needs. This implies that a cultural change from data"ownership" to data "trusteeship" may be required. • The data trustee will be responsible for meeting quality requirements levied upon thedata for which the trustee is accountable. • It is essential that the trustee has the ability to provide user confidence in the databased upon attributes such as 'data source.' • It is essential to identify the true source of the data in order that the data authoritycan be assigned this trustee responsibility. This does not mean that classified sourceswill be revealed, nor does it mean the source will be the trustee. • Information should be captured electronically once and immediately validated asclose to the source as possible. Quality control measures must be implemented toensure the integrity of the data. • As a result of sharing data across the Government, the trustee is accountable andresponsible for the accuracy and currency of their designated data element(s) andsubsequently, must then recognise the importance of this trusteeship responsibility.

PR-DP-4 Common vocabulary and data/meta-data definitions.	
Statement	Data is defined consistently throughout all levels of Government, and the definitions are understandable and available to all users.
Rational	• The data that will be used in the development of applications must have a common definition throughout the Service to enable sharing of data. • A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.
Implications	• Significant energy and resources must be committed to this task. It is a key to the success of efforts to improve the information environment. • The Government shall establish the initial common vocabulary for the business. The definitions will be used uniformly throughout the government units. • Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the corporate "glossary" of data descriptions. • Ambiguities resulting from multiple parochial definitions of data must give way to accepted Service wide definitions and understanding. • Multiple data standardisation initiatives need to be coordinated. • Functional data administration responsibilities must be assigned.

9.6 Technology Principles

PR-TP-1 Manage technical diversity.	
Statement	Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.
Rational	• Limiting the number of supported components will simplify maintainability and reduce costs. • The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements.

	• Common technology across the enterprise brings the benefits of economies of scale to the enterprise. • Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.
Implications	• Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle. • Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced. • Enterprise is not freezing its technology baseline. Enterprise should welcome technology advances and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated. • The Technology product portfolio that is utilised for common/transversal systems is reduced toa finite manageable set that will strike a balance between the ease and cost of managingthe life-cycle of technology on the one side, andstimulating healthy economic competition andgrowth of the ICT industry • The Technology product portfolio that is utilisedfor departmental unique systems is reduced toa finite set per department. This will allow eachdepartment to reduce the complexities per department, but also to have different technologyportfolios from each other that will enable faireconomic participation of the ICT industry. • Growing and evolving the ICT portfolio requirethat emerging, innovative or cutting-edge ICTproducts must be monitored on a continued basis;and be subjected to proof-of-concept to test forrelevance, compliance and impact to governmentoperations before it is introduced into ICT productportfolio. • The efficacy, efficiency and risk of the existing ICT product portfolio are reviewed on a regular basis to identify candidate products that need to be upgraded or disposed.

PR-TP-2 Adopt standards and best practices.	
Statement	Designing and defining business processes, information systems, technology products and services used by ministries/agencies should adhere to industry standards and open architectures. The Government should employ formal practices, methods and tools for all stages.

	It should encourage to use standard protocols/formats to communicate between data, applications, and technology in project architecture Open Standards are adopted in the design and implementation of all greenfield systems. Legacy systems are incentivized to migrate to open standards, where required.
Rational	• Standard protocols will provide flexibility when there is need to change some element in architecture • Using viable open standards will improve services to the community through better interoperability ingovernment, greater flexibility and by reducing risk for government • Adopting standard methodologies will ensure quality assurance, repeatability and consistency for business projects with an IT component • Adherence to industry specific best practices will ensure that services are being delivered in optimal way
Implications	• This will reduce the overhead cost of developing systems • The quality reuse of business information and processes will be possible with regular checks formonitoring • Use of standard methodologies will ensure process information interoperability and ease to reuse • It will avoid reinventing the wheel as existing research on industry best practices will be reused

PR-TP-3 Future proof.	
Statement	Enterprise Architectures are suitably designed and developed so as to be future-proof, not requiring frequent revisions with the advent of every new technology.
Rational	Principles should be enduring, yet able to accommodate changes. Technologies change rapidly and EA should accommodate such new developments. Though may be expensive at the start, the life-time cost of acquiring future-looking technologies will be lower than sticking to older technologies for which the Government may not even get support.
Implications	• Technolog projects should give priority to (elsewhere) tested and confirmed futuristic technologies. • Replacing legacy systems with new systems is encouraged within the EA framework.

PR-TP-4 Shared infrastructure.	
Statement	IT Infrastructure is shared to ensure optimal utilization and effective maintenance.
Rational	This principle promotes shared infrastructure to reduce costs and improve information flows.
Implications	• A single uniform network infrastructure allows an enterprise to respond more efficiently when faced with requests by MDAs for WAN component upgrades and installation • A centrally developed and managed infrastructure provides a more cost-effective use of infrastructure resources • Focus WAN requirements on functional specifications such as level of service needed, throughput needed, and response time needed. The implementation of an appropriately responsive WAN is a specialised function performed for the enterprise in its entirety.

9.7 Security Principles

PR-SP-1Security by design.	
Statement	Security must be built into all stages and all aspects of architecture development. Security concerns extend to all the IT activities of the enterprise.
Rational	• Open sharing of information between ministries/agencies and the release of information via relevant legislation. • Data sharing must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.
Implications	• Applications are secure by design and developed using secure coding standards and practices. • Security must be designed into data elements from the beginning; it cannot be added later. • Systems, data, and technologies must be protected from unauthorized access and manipulation at all ministries. • Well defined access controls and access constraints must be designed into the centralized metadata repository based on the need of business services owned. • Data is protected from loss, unauthorized use and corruption, through adoption of international standards and best practices, duly protecting the privacy of personal data and confidentiality of sensitive

	data.

PR-SP-2 High availability and disaster recovery.	
Statement	Technology architecture component and services should be deployed and configured in high available mode to provide maximum availability to business services. Business services and IT components/infrastructure should be operational in spite of primary IT Infrastructure failures and interruptions due to any disaster.
Rational	• Information services are critical to the success of business functionality. Extended periods of service unavailability or loss of identity data could have severe negative impacts. • It eliminates single point of failure and provide high availability for business services/application • Protocol and technologies such as HACMP (High Availability Clustering Multi Processing), VRRP (Virtual Router Routing Protocol) and GLBP (Global Load Balancing Protocol) etc can be used to maintain high availability of the system/IT Infrastructure
Implications	• Maximum availability of business services, which is deployed on redundant or HA (High Availability) configured IT Infrastructure • Design documents and implementations plans detail how the service was designed in order to meet or exceed its availability and recovery goals. Recovery procedures are documented for each service. • RTO (Recovery Time Objective) and RPO (Recovery Point Objective) will define the time and service level for restoration of services after disruption.

9.8 Integration Principles

PR-IP-1 Interoperability.	
Statement	Interoperability is assured through adoption of open standards and open interfaces.
Rational	Identify common components (including existing Government policies, standards, application, technology etc. wherever relevant) across the interoperability domain and define policies, standards, and procedures to ensure reusability of artefacts. For e.g. defining data structure, data sets at a

	national level etc. Choose standards that will enable more choice and reduce the administrative burden.
Implications	• Eliminates patchwork of ICT solutions in different government offices those are unable to -talk or exchange data. Interoperability allows seamless exchange of information, reuse of data models and inter-changeability of data across systems • Brings in the ability to effectively interconnect, collaborate, access and facilitate data Integration in order to communicate between different government organizations (G2G, G2C, and G2B etc.).

PR-IP-2 Openness and transparency.	
Statement	Government data, applications, and technologies are made open through the adoption of open standards, barring exceptions, so thatexternal parties can build services.The architectural decisions taken are also transparent to all stakeholders.
Rational	This principle holds that adherence to open standards should be promoted as it will enable all stakeholders to get access to government data and applications within the limits of security and privacy. Architectural decisions shall also be transparent to make the system dependable and trustworthy.
Implications	• Adherence to standard that will provide for choice of vendor will promote competitiveness and opportunity to look at cross platforms. • The attributes of open standards such as platform independence, vendor neutrality and ability to use across multiple implementations and the model for establishing open standards are whatwill allow for sustainable information exchange, interoperability, flexibility, data preservation & and greaterfreedom from technology and vendor lock-in. • The governance structure as well as processes and tools will be transparent to all stakeholders allowing feedback and improvement.

PR-IP-3 Primacy of citizen experience.	
Statement	All service interactions are designed with citizens at the core, byproviding integrated multi-channel service delivery
Rational	The government exists to serve the public who want simpler, faster, better and cheaper access to government services and information.

Implications	• Government services, and systems supporting the delivery of these services, should be designed, or re-designed, to operate in a way that is user-centred and intuitive to use and access and which facilitates rather than inhibits service delivery. • MDAs will design and apply their business processes and services to benefit citizens, even when the services cross lines of business. • The government offers citizens a single, -unified- face, reducing duplicate, needlessly complex, inconsistent ways of using government services. • Citizens can access government services through various means.

PR-IP-4Integrated multi-channel services.	
Statement	Integrated Services that cut across MDA-silos are identified, designed and delivered through multiple delivery channels.
Rational	One of the aspirational goals of ENEAF is to support the achievement of Unity in Diversity. This is made possible inter-alia through provision of Integrated Services, obviating the need for the citizens/ businesses to interact with multiple Government agencies to achieve their objective.
Implications	• Good application delivery enables a high level of system integration • Reuse of components, and rapid deployment of applications in response to changing businessrequirements. • Multilingual and inclusive efforts will take centre stage. • Citizens can access government services through various means.

Ethiopian eGovernment Interoperability Framework (EeGIF)

Governance and Compliance

School of Information Science (AAU)
MINISTRY OF INNOVATIONS & TECHNOLOGY | ADDIS ABABA, ETHIOPIA

Document Description

Document Title	Ethiopian eGovernment Interoperability FrameworkGovernance and Compliance
Document version	0.1
Document Status	**Draft**
Author(s)	Ermias Ababe Mesfin Kifle (PhD) Tibebe Beshah (PhD) Wondwossen Mulugeta(PhD) Workshet Lamenew (PhD)
Decision	under Review

Version Control

Version	Date	Description of changes made
0.1	03/11/2019	Draft Document

Document Validation

Version	Authors	Reviewed by	Date	Status
0.1	ERMIAS ABABE MESFIN KIFLE (PHD) TIBEBE BESHAH (PHD) WONDWOSSEN MULUGETA (PHD) WORKSHET LAMENEW (PHD)		03/11/2019	DRAFT

List of Acronyms

CIO	Chief Information Officer
DRM	Digital Rights Management
EA	Enterprise Architecture
eGIF	Electronic Government Interoperability Framework
EeGIF	Ethiopian Electronic Government Interoperability Framework
ENEAF	Ethiopian National Enterprise Architecture Framework
EPAN	European Public Administration Network
FDRE	Federal Democratic Republic of Ethiopia
G2G	Government to Government
G2E	Government to Employee
G2C	Government to Citizen
G2B	Government to Business
GC	Governing Council
ICT	Information and Communication Technology
MDA	Ministry, Department, Agency
MInT	Ministry of Innovation and Technology
NDC	National Data Center
PMO	Prime Minister Office
SLA	Service Level Agreement
TWG	Technical Working Group
UNDP	United Nations Development Programme
XML	eXtended Mark-up Language

Table of Contents

1 Executive Summary

This document presents the proposed governance framework of the EeGIF which is an extension of the ENEAF by focusing on the issues that are pertinent to interoperability. Issues of compliance is also given focus on this document where issues like trigger of compliance checking, compliance confirmation processes, consequence on non-compliance are outlined.

The other relevant element of compliance, which is the underling policies are categorized into general, data, security and technological polices are elaborated. As an additional element, the principles of interoperability, with the required linkage with the driving NEAF principles are elaborated. This governance and compliance document also contain a high-level compliance checklist that can be extended and used to develop compliance template.

LIST OF TABLES

2 EeGIF Governance

The government ecosystem is preferred to work in a coordinated manner to maximize efficiency and assist ease of doing business. The long- and medium-term reform roadmap of the Federal Democratic Republic of Ethiopia (FDRE), published by the Prime Minister Office, edify that business processes in the area of starting business, paying taxes, various license and permission processing, property registration, etc. shall be greatly done via electronic and online services. Such ambitions will only be met with the proper governance of electronic governance in general and interoperability in particular.

Thus, in an attempt to use shared resources and data, interoperability has been identified as a major issue to be addressed by every e-government agency. An interoperability framework aims to provide the basic standards and working methods that every ministry, agency, commission or organizational unit which is relevant for the e-government strategy implementation should adopt. Criteria for selection and inclusion of standards in an interoperability framework are crucial, since they influence the utility that the framework delivers to the e-government agencies. In this regard, the governance of eGIF plays a crucial role.

The United Nations Development Programme (UNDP), in its 1997 policy paper defined governance as "the exercise of economic, political and administrative authority to manage a country's affairs at all levels. It comprises the mechanisms, processes and institutions through which citizens and groups articulate their interests, exercise their legal rights, meet their obligations and mediate their differences"[1]. It is also defined in various literature as the *exercise of power or authority by political leaders for the well-being of their country's citizens or subjects*. It is the complex process whereby some sectors of the society exert power, and enact and propagate public policies which directly affect human and institutional interactions, and economic and social development. The power exercised by the participating sectors of the society is always for the common good, as it is essential for demanding respect and cooperation from the citizens and the state. Governance mechanisms ensure that government meets the needs of a community of stakeholders by providing a clear pathway to gaining endorsement of decisions by authorities.

[1] *United Nations Development Program, Governance for sustainable human development, UNDP policy document, New York, 1997.*

Thus, interoperability governance, following the European Public Administration Network (EPAN): "is concerned with the ownership, definition, development, maintenance, monitoring and promotion of standards, protocols, policies and technologies" [2].

More specifically and when contextualized to eGovernance, interoperability governance it is the use of authority to make sure that electronic and information communication technology policies, processes, procedures and standards are produced, disseminated, implemented and assessed properly. In this regard, the stakeholders for such governance is bound to the scope of the ecosystem. As the most dominant coverage, the scope of eGIF is expected to be applied for:

- ✓ The ***Government to Government (G2G)*** e–Government: The objectives of G2G are to improve the cooperation and collaboration between governments of different physical locations and levels. This type of e-government has the role of guaranteeing the integration of systems and sharing of databases of local or federal governments. It also has to ensure the cooperation and collaboration through enforcement of laws, public safety and emergency management.
- ✓ The ***Government to Employee (G2E)*** e-government: This type's goal is to ensure and enhance the effectiveness of government administration, internally, as well as its efficiency. The role it has to play is to organize the internal operational processes to implement and adopt the best practices in governance. Regarding the administration employees, it has to provide services such as training, payroll management.
- ✓ The ***Government to Citizen (G2C)*** e-government: has the role to improve the quality of services provided to citizens and the relationship between government and citizen. This is done by proving access to information varying from general information to specifics such as information on education and learning, policies, and loans.

[2] *European Public Administration Network eGovernment Working Group (2004). Key Principles of an Interoperability Architecture. http://www.reach.ie/misc/docs/PrinciplesofInteroperability.pdf].*

- ✓ The ***Government to Business (G2B)*** e-government: aims to provide services of better quality to businesses like eradicating duplicated data and reducing the cost of transactions.

The compliance with the EeGIF cannot be imposed on citizens, private businesses and foreign governments, but the Federal Republic of Ethiopia can make it available to all so that interoperability can be enhance if required by these parties.

The governance should be designed based on the stages of development and maturity of eServices and engagement by the nation. According to the gap analysis and assessment survey done, various organizations provide services which falls in at least the four early stages. Putting Ethiopia in any of the stages makes it difficult as the service provision is not consistent with the requirements outlined in the five stages and some, in fact, provided a transactional service without achieving the interactive or enhanced level. The United Nations defined a five stages model for e-government, namely:

- ✓ **Stage 1 Emerging**: - In this stage, the government is present online through websites by providing static information for users; they are mainly official information about universities, government ministries, departments and agencies.
- ✓ **Stage 2 Enhanced**: - In the enhanced stage, the websites become dynamic, updating data frequently and providing links for users to archived information
- ✓ **Stage 3: Interactive**: - The online presence becomes more interactive; users are able to download documents such as application forms for passports, and car license.
- ✓ **Stage 4 Transactional**: - The transactional stage takes the online government to a further level by allowing the users to upload documents such as applications for car license, or passport, as well as making online transactions like paying taxes online, and doing e-banking.
- ✓ **Stage 5: Connected**: - In the last stage, all government services are available online and accessible through a one-stop portal. At the portal, all the government services are integrated. In Connected stage, the expectation Is that:
    - o horizontal integration, which is among government agencies
    - o vertical integration between local and central agencies of the government
    - o connection between the government and its citizens
    - o connection between all the players from government, private sector, academic institutions and civil society

2.1 Governance Principles

Providing the guiding principles for the establishment of the governance is as important as the elements of governance. Accordingly, based on the benchmarking and experience from other countries, the following principles are taken to underpin the governance of the eGIF and its operation:

1) The eGIF is driven by the Ethiopian National Enterprise Architecture Framework;

2) Sufficient and adequate resources and capabilities shall be deployed to support the governance arrangements;

3) The maintenance and update of the EeGIF document will be through the eGovernment technical working groups to be established under the governing council;

4) The governance arrangements must be consistent with both current and future legal requirements;

5) The governance arrangements will build confidence in, and commitment to, the eGIF from all its stakeholders;

6) With regard to the day-to-day operation of the EeGIF, the governance arrangements will show a close fit with the responsibilities and capabilities of the organizations involved which is depicted on the governance structure;

7) The governance arrangements must account for the complexity of e-government stakeholders and operating environments.

8) MDAs that are required to adopt the EeGIF will be given the opportunity to participate in its governance as the main stakeholders;

9) The collective interests of government should be balanced with the interests of individual MDAs and their stakeholders. Where this is not possible, the collective interest should be given the greater priority.

2.2 Structure and Duties

2.2.1 Overview

Governance, in general, entails two processes:

I. ***decision-making*** **and**

II. ***implementation of the decision.***

The *decision-making* refers the process by which an authority who looks into various aspects and makes the decision on what to put in place as a government entity, guided by socio-political structures. Likewise, *implementation* is the process of performing the required action that follows the decision; it entails the actualization or materialization of the plan or decision. Governance is not just decision-making because decision without implementation is self-defeating. Thus, the two processes necessarily go hand-in-hand in, and are constitutive of, governance. Accordingly, the structure based on which the decision is made and the implementation is executed is vital.

The recommendation of European Public Administration Network (EPAN), which is also found to be convenient in Ethiopian case, that a single agency like MInT should be responsible for technical and semantic interoperability aspects of the eGIF. Accordingly, MInT should have the following characteristics and should be:

- ✓ Separate from all sectoral domains to ensure independence;
- ✓ Seen as expert in the field of interoperability to engender trust;
- ✓ Capable of working as a collaborative partner with fulfilment agencies and sectors;
- ✓ Proactive in the promotion of standards and their use;
- ✓ Responsible for monitoring usage of and policing adherence to standards, guidelines, policies and protocols;
- ✓ Singularly focused on standardizing and providing interoperability on public service; and
- ✓ An advisory and collaborative body to fulfilment of MDAs in developing strategies, implementing solutions, coordinating cross-agency aggregated services and to communities of practice in setting and publishing standards.

2.2.2 Structure

Structure is an arrangement and organization of interrelated components in a system are organized to achieve the organizational objectives. Showing the power

of authority, the levels and the interaction will help in accomplishing goals. Thus, establishment of the correct organizational responsibilities and structures to support the framework and the governance processes is vital. In light with this, after reviewing the mistrial structure and consultation with relevant bodies, the following governance structure with the associated duties and responsibilities along with membership suggestions are proposed. This EeGIF governance structure, is powered by the ENEAF governance structure developed by the project members.

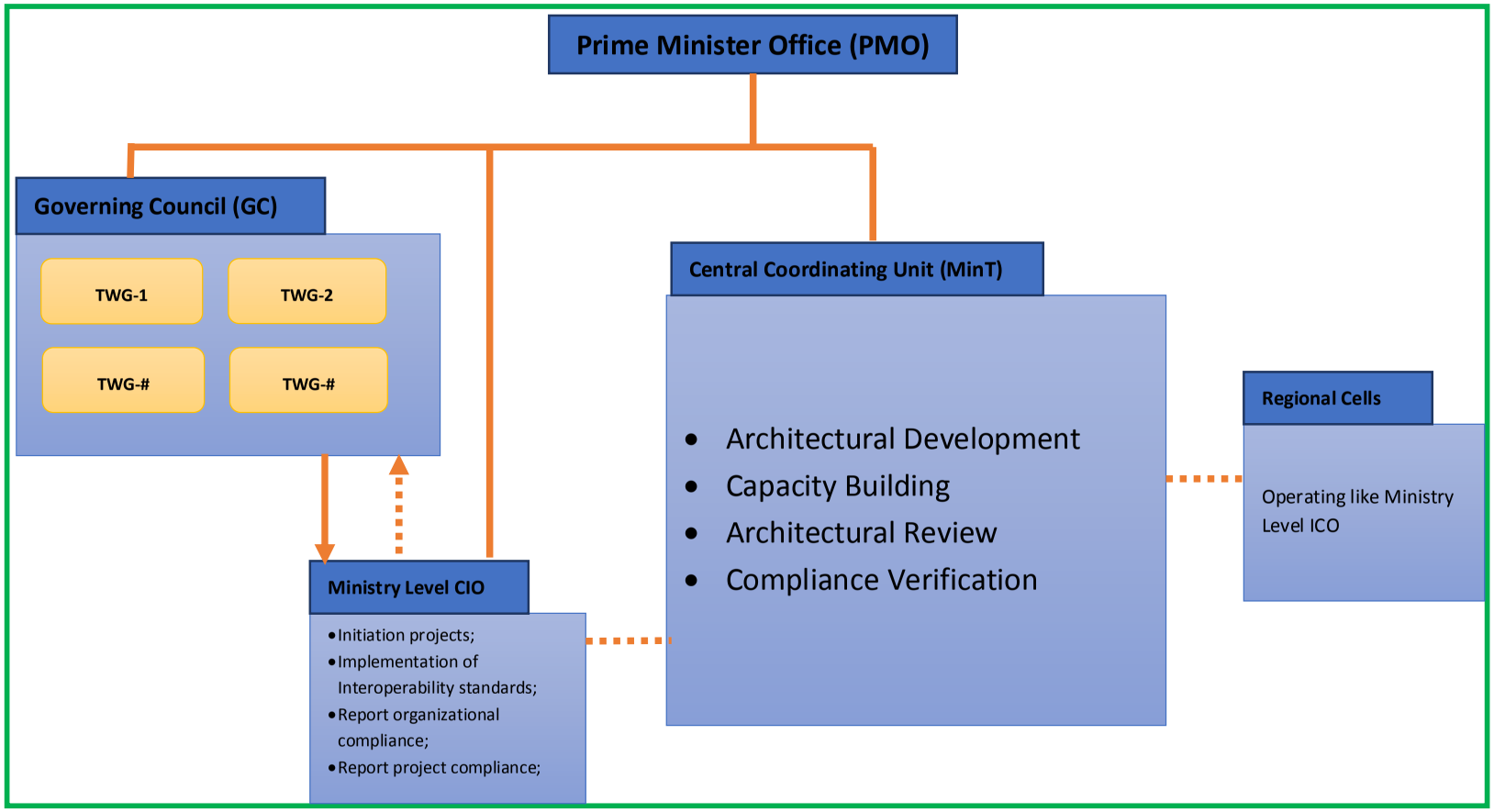


Figure 1: Proposed ENEAF and EeGIF Governance Structure

2.2.3 Duties and Responsibilities

A) Governing Council (GC)

The Governing council is the highest body for decision making of ENEAF and EeGIF related activities. The council is responsible for overseeing and supervising the entire process of cross-organizational e-Service delivery in line with the digital transformation plan. The Committee shall work to ensure all standards are complied with.

Membership

- ✓ Headed by Delegate from the PMO
- ✓ State Minister of MInTwill be the Secretary
- ✓ Members: State Ministers of
  - ➢ All Ministries Represented by their CIOs or equivalent
  - ➢ Attorney General
  - ➢ Three Private Sector Representatives
  - ➢ Donor Representatives
  - ➢ Representatives from Professional Associations
  - ➢ Representatives Higher Learning Institutions

Roles and Responsibilities:

1. Topics and decisions of the Council are to be prepared by the Secretary.
2. The council should approve all strategic initiatives in the field of IT developments of the ministry:
   - ✓ Take decisions and responsibility of reengineering processes needed for the implementation of new projects.
   - ✓ Meet annually to assess the compliance level of stakeholders with the provision of the framework.
   - ✓ Coordinate (where necessary) or assist in the development, promotion and adoption of standards, guidelines and policies that will help ensure the actualization of the purpose of this framework.
   - ✓ Coordinate the review and update of the framework in line with the provision the EeGIF.
   - ✓ Envision and serve as decision-making arm the execution arm
   - ✓ Provides guidance and assistance to the government ministries and agencies and enable them to enhance EA maturity

- ✓ Guides the development of EA reference models, repository and detailed standards at national, federal and regional levels identified in the roadmap
- ✓ Reviews and approves documents generated by the chief architect
- ✓ Meet annually to assess the compliance level of stakeholders with the provision of the ENEAF.

B) Technical Working Group (TWG)

Various Technical Working Group shall be formed by and from the members of the Governing Council who will be responsible for formulation, revision, monitoring and actual implementation of the EeGIF and report to the GC as and when required. The TWG could also have members from specific domains to assist in accomplishing its duties after approval from the GC.

C) Central Coordination Unit (MInT)

The Central Coordination Unit is the responsible unit under MInT who will be tasked with the responsibilities of devising, enacting, drafting, enforcement and monitoring of the eGIF.The central coordinating Unit will mainly be responsible for:

a. Architectural Development
b. Architectural Review
c. Capacity Building
d. Compliance Verification

Roles and Responsibilities:

1. Responsible for ICT strategy planning, implementation and supervision processes. Dealing with public relations on information society issues;
2. Has a right to get information from government bodies about the use of ICT systems and about the results of systems development processes;
3. Responsible for drafting the ICT budget in the state budget in cooperation with the Ministry of Finance. The Unit supervises the most important development projects which might also look into the compliance to EeGIF;
4. Responsible for coordination of drafting of the main ICT-related legal acts. The Unit should have a right to present opinions and approve all ICT-related legal acts which could be initiated by the appropriate ministry;
5. Monitors the compliance of the reference models and standards;
6. Checks interoperability across platforms and services;
7. Ensures cost effective implementation of EeGIF and standards;

8. Ensures consistent integration among ministries and agencies;
9. Ensures improved and optimized resource utilization;
10. Has the right to initiate new ICT-related legal acts;
11. Responsible for management of the work of CIO working groups, planning and implementing CIO training activities;
12. Coordinates international cooperation activities in the field of ICT. Often international cooperation is performed in other ministries (e-health issues – Ministry of Health, basic ICT infrastructure issues – Ministry of Innovation and Technology, etc.) but the central coordination should be performed by the Central Coordination Unit;
13. Initiates cross-government projects and programs;
14. Responsible for general guidance, recommendations and standards;
15. Prepares EA and standards learning packages;
16. Organize training for stakeholders;
17. Create links with Vendors, Academic institutions and IT professional associations for preparation of trainings, learning materials, and organize certifications, and
18. Any additional and related responsibilities laid on the Central Coordinating Unit by the Governing council.

D) Ministry Level Chief Information Officer (CIO)

The Central Coordination Unit needs to have contact points in ministries to cooperate with them for the introduction, operation and monitoring or the EeGIF. CIOs or Directors of ICT or any equivalent personnel should be nominated at the ministry level (normally he/she should be at the level of a Head of Department or an advisor to the ministry) with the following responsibilities:

Roles and Responsibilities:

1. Create and implement ICT action plan at the ministry level in line with the EeGIF standards;
2. Work towards achieving EeGIF compliance of the MDA and information systems projects;
3. Plan and prepare for approval the annual ICT budget for the ICT Council of the ministry. The ICT budget should be in line with both the

government ICT action plan and the ministerial action plan which considers the compliance requirements;

4. Implement different projects, which are approved of their EeGIF compliance, related to procurement, supervision of projects, ICT training issues of ministries, etc.
5. Organize ICT systems maintenance and user help desk;
6. Organize capacity building on EeGIF, ENEAF, standards and the required compliance;
7. The CIO should be a member of the ICT workgroup of CIOs of ministries led by the head of the Governing Council;

E) Regional Cells

The Regional Cells, based on the federal structure of the Federal Democratic Republic of Ethiopia, will act like Ministry level CIOs and collaborate with the Central Coordinating Unit (MinT) for initiation, planning, execution, monitoring, capacity building and compliance on EeGIF related matters.

3 Policies

In the process of soliciting the policies required for the operationalization of the EeGIF, it was found that the policies identified on the 1st version of the EeGIF are relevant and well-articulated. These policies are reorganized and presented as follows with minor modification. Figure 2 presents the relationship between the general polices and the three pillars of policies for interoperability along with the concrete elements to be addressed under each policy issues. The description after Figure 2 outlines, in detail, the policy issues under the four major categories:

- General Policies;
- Data and Metadata Policies
- Security Policies
- Application and Technology Policies

It has to be noted that the required standards and polices with most of these policy points are crafted on the Standards document of the proposed Ethiopian eGovernment Interoperability Framework.

Figure 2: Policy Frame

3.1 General Policies

- ✓ Standards and Procedures should be based on the objective, scope and principles of EeGIF;
- ✓ Adopt objective, principles, policies and standards as a respective ministry/agency's policies and institutionalize the same across all government departments through passing a mandate in the cabinet/parliament.
- ✓ Any policy and standard defined in EeGIF should be consistent and compliant with the existing Government policies and standards wherever relevant.
- ✓ The use of open standards should be given preference over proprietary standards wherever appropriate. In the event of choosing proprietary standards the EeGIF principles should be considered as the basic requirement.

- ✓ The institution-based approach should be replaced by a service-center one closely aligned with eGovernance strategy and adherence to the eGIF should be mandated throughout all government ministries, agencies and authorities.
- ✓ In case of private public partnership, the standards for information exchange between the private partner and the government should comply with the EeGIF but flexibility may be allowed in the information exchange between the partner and the distribution network of the partner reaching the citizens/consumers.
- ✓ Whenever a new version of EeGIF is released, it is mandatory to train the working group committee members who should in turn be mandated to train the concerned/identified IT resource in each government department across all ministries/agencies/authorities.
    - All ministries/agencies/authorities should review their technology implementations against the EeGIF, whenever a new/enhanced/revised version of the eGIF is released or whenever they are looking out for new implementations, upgrade of legacy systems and reviewing their e-Governance/e- Services strategy.
- ✓ All ministries/agencies/authorities should recommend compliance to EeGIF in their bidding process for any technology product/service procurement.
- ✓ All standards should first apply to new systems and then move on to incorporate the standards onto the legacy systems during upgrades.
- ✓ The systems in each ministry/agency/authority that are built to support a given access device should comply with the specification given in the EeGIF standards.

3.2 Application and Technology Policies

- ✓ The standards should as far as possible be aligned with the world wide web for all public sector information systems.
- ✓ The development of applications or e-Services should provide services to the users who do not have the access to latest technologies and to those who may not be aware of using such technologies.
- ✓ While developing applications, special accessibility needs have to be considered including the provision of more sophisticated, and user-specific resources.
- ✓ Current applications may not need to comply immediately with EeGIF; however, any new information system/change/upgrade must be compliant. A given version of eGIF should apply over the lifecycle of a specific, discrete system. It is desirable to move upgrade/re-engineer the system up to the most recent version of the framework. In

case it is not possible to comply, an appeal for exemption must be approved by the Governing council.

- ✓ All future application and migration of legacy application should be web based (browser-based interface).
- ✓ Email communication should be recognized as the official communication and Email should be the preferred medium of official communication.

3.3 Data and Meta Data Policies

- ✓ XML should be the primary standard for data integration and data management for all application in every ministry, agency and authority in Ethiopia. The Ethiopian Meta data standards should be primarily based on the international Dublin Core model.
- ✓ Development of national level data set and centralization of Meta data of the country should be done in compliance with the interoperability standards on metadata.
- ✓ The working groups and experts should develop guidelines for XML Schemas that will be used for all new applications. These guidelines should include mandatory requirements for XML Schema structure and content.
- ✓ Data standards, data exchange standards, integration standards are interrelated, their compatibility and technical requirements should be considered.

3.4 Security Policies

Security policies are required in order to ensure:

- ✓ Confidentiality/privacy of Ethiopian government held information
- ✓ to continue to exercise control of Ethiopian government data and computing environments
- ✓ Protect confidentiality rights accorded to personnel who use government systems
- ✓ Ensure privacy of personal information.
- ✓ Ethiopia should have process, principles, policies, technology and control mechanism to achieve fair maturity in Trusted Computing and Digital Rights Management (DRM).
- ✓ Security is a process that should be present at all stages of application development, the security working group should document systems, security controls, and the environment topologies, educate every ministry/agency IT department on their responsibilities for the security and the correct use of the access means and update policy and procedures

- ✓ The security requirements for the information, the services, and the infrastructure should be identified and treated in accordance to the type of information, SLA's, and the outcome of the risk analysis.
- ✓ To start with, the existing security policies should be enforced across all ministries. The policy document should be updated and maintained eventually. Key procedures pertaining to the following areas should be implemented and enforced
    - Application Acquisition, Development and Maintenance Procedure
    - Audit Logging Procedure Version
    - Backup and Restore Management
    - Capacity Management
    - Change Management
    - Incident Management Procedure
    - Information Labelling and Handling
    - Physical Access Process
    - Physical Access to Secure Areas Process
    - Physical Zoning Guidelines
    - Risk Assessment Methodology
    - User account management.
- ✓ The security policies, procedures and standards should be enforced to protect the privacy of data. Suitable media should be used to store/transport/process in providing the adequate level of protection needed.

4 Principles

Government initiatives are built on the principles that are put forward by the authorities responsible to initiate or implement the initiatives. As per the assessment made and the benchmarking or mix of countries these principles are driven by the priorities set by the government and the landscape of the international ICT development. This should be aligned with the development goal of the country as ICT influences all sectors. Based on these priorities and goals, a set of directions are required to define the kind of policies and for selection of appropriate standards.

Principles typically provide the basic justification for the need of the specific policies/standards including the standards to be used. The principles also reflect concerns,

risks, changes and related issues of eGIF. The principles cover parameters for selection of standards and also cover the limitations of the organization, anticipated outcomes of the eGIF, requirements for project and operational management, and governance. Principles also outline a guidance on future versions of the initiative. Principles are applicable and essential to interoperability or architecture. Figure 3 shows the categorization of the principles of EeGIF in line with the pillars of interoperability.

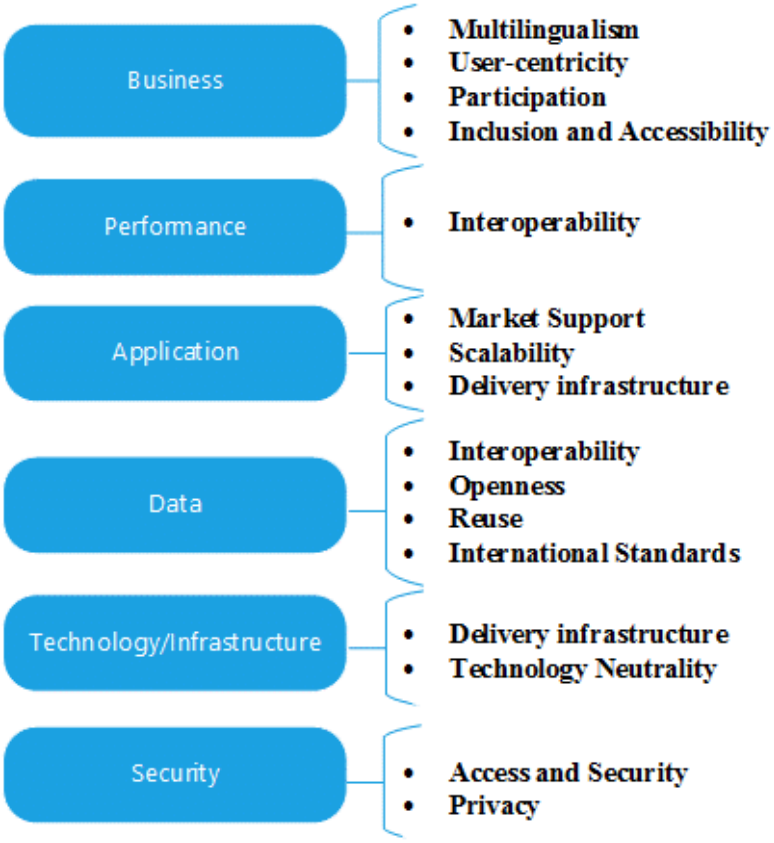


Figure 3: EeGIF Guiding Principles

Based on the assessment of Ethiopia's current environment, estimation of future requirements, and leading practices of Government Interoperability Framework of the various countries, the following key principles have been suggested for EeGIF. The major principles are derived from the ENEAF document, which is part of the overall eGovernment document, where the specific principles from which these particular eGIF principles are elaborated from are indicated. For additional information on the referred principles, readers are advised to consult the principles section of the ENEAF document.

Interoperability	
Statement	The basic premise of this principle is to ensure that policies should reinforce and standards selected should facilitate interoperability;
Driving ENEAF Principle(s)	PR-IP-1: Interoperability PR-DP-2: Data is shared PR-BP-1: Unity in Diversity

Openness	
Statement	The attributes of open standards such as platform independence, vendor neutrality and ability to use across multiple implementations and the model for establishing open standards are what will allow for sustainable information exchange, interoperability and flexibility. Open standards could include open source as well but it is not necessary that all open standards are open source. In addition, it entails that the specifications are documented and available to the public;
Driving ENEAF Principle(s)	PR-IP-2: Openness and transparency PR-AP-2: Technology and independence

International Standards	
Statement	Preference will be given to standards with the broadest remit, so appropriate international standards will take preference over local and regional standards;
Driving ENEAF Principle(s)	PR-TP-2: Adopt standards and best practices

Reuse	
Statement	This principle propagates sharing, re-use and collaboration and essentially highlights the importance of identifying common components across domains
Driving ENEAF Principle(s)	PR-TP-4: Shared infrastructure PR-AP-1: Sharing and reusability

Market Support	
Statement	The specifications selected are widely supported by the market, and are likely to reduce the cost and risk of government information systems
Driving ENEAF Principle(s)	PR-BP-1: Maximise benefits to the Government

Scalability	
Statement	The principle suggests that the standards chosen should meet the changing and growing ministry and agency's needs and requirements and the applications and technologies should essentially scale up, adapt and respond to such requirement changes;
Driving ENEAF Principle(s)	PR-TP-3: Future Proof

Privacy	
Statement	Guaranteeing the privacy of information with regard to citizens (e.g. health records), business (e.g. organization statistics) and government (e.g. confidentiality agreements) to enforce the legally-defined restrictions on access & dissemination of information
Driving ENEAF Principle(s)	PR-SP-1: Security by design

Participation	
Statement	Platform for participation by allowing diverse participation and engagement to ensure that interests of direct and indirect stakeholders have a chance to be represented as much as possible;
Driving ENEAF Principle(s)	PR-GP-3: Transparency PR-BP-1: Unity in Diversity

Access and Security	
Statement	Subscribing to principles of universal access and security to support a global competitive market and the compatibility of new technologies within growing interdependent systems.
Driving ENEAF Principle(s)	PR-SP-1: Security by design

Delivery infrastructure	
Statement	Channels are interface through which integrated public services are delivered. Services should be offered in both an online and offline mode. Digital services should be based on open standards and accessible on all devices and platforms. Personal information should be protected. Citizens must all be provided with digital addresses/identities to allow government to engage with them directly. Centralized coordination to ensure interoperability is required;
Driving ENEAF Principle(s)	PR-BP-3: Integrated multi-channel services

User-centricity	
Statement	Supporting the needs of citizens and businesses in a secure and flexible manner.
Driving ENEAF Principle(s)	PR-IP-3: Primacy of user experience

Inclusion and Accessibility	
Statement	Equal opportunities should be created for access to public services through open and inclusive services, on all devices and platforms, to all citizens without discrimination, including gender, religion, ethnicity, colour, persons with a disability, and the elderly.
Driving ENEAF	PR-BP-1: Unity in Diversity

Principle(s)	

Multilingualism	
Statement	Information systems for the public service should support multilingualism in support of the usability by people from different regions with different language capabilities as it applies to all government organs;
Driving ENEAF Principle(s)	PR-IP-3: Primacy of user experience

Technology Neutrality	
Statement	Services should be provided through interfaces that are technology and vendor agnostic.
Driving ENEAF Principle(s)	PR-AP-2: Technology and independence

5 Compliance

Compliance focuses on the mechanism of confirming whether an organization meets the requirements to be labelled as fit with respect to some rules and procedures. For interoperability, compliance is mainly focused on evaluating if a ministry, agency, commission or any relevant government unit is fulfilling the requirement. For interoperability to be effectively achieved, there have to be a coherent alignment between the eGIF policies and standards and the systems implemented at the MDAs. Therefore, there is the need to test for compliance and this is done by checking whether or not the MDA systems in place or to be implemented conform to policies and standards listed in the eGIF. To be eGIF compliant, a system should satisfy both requirements. Without compliance interoperability cannot be achieved.

Directing agencies and ministries to adopt and comply with policies or procedures towards eGIF is important, it does not provide the guarantee that it will be operational. The scope of the eGIF and how it was developed will affect its compliance. Putting additional enforcement methods is found to work greatly towards wider compliance. In addition, deciding on the scope of implementation could also help in this regard. For

instance, enforcing the eGIF only on new information systems implementation and then moving to legacy systems or vice versa can be exercised.

Many countries are also following an incentives-based approach to eGIF compliance where budget provision for new information communication technology projects are linked with eGIF compliance. This means only eGIF compliant e-government projects will receive new funding. This is particularly effective if all ICT projects are funded centrally and the eGIF lead agency has effective control over the use and disbursement of this fund. To make this practical, there is a need to have a procedure where agencies and ministries produce compliance certificate from MInT in the process of securing fund for their projects. In this scenario, non-compliant projects will not be funded by government. While there is a need to develop detailed and measurable compliance checklist, the general issues to be included in compliance checklist and their categorization ad presented as annex (*Annex A: Interoperability Compliance Checklist*). The governing council should develop a detailed compliance checklist through one of the TWG to be established.

5.1 Triggers for Compliance Checking

The time at which MDAs looks into the eGIF and the compliance requirement are one of the main phases in the process of putting the framework into action. Accordingly, all MDAs, who will be expected to comply with the eGIF, should review their implementations or current organizational status against the eGIF whenever:

i) they are planning to have organizational compliance certificate or update;
ii) they are planning new information systems implementations;
iii) they are planning to undergo upgrade or update of existing or legacy systems;
iv) a new version of the eGIF is released

5.2 Compliance Responsibility

The ultimate responsibility for compliance rests with the CIO or information technology directorate of the MDA. These experts are expected to ensure that compliance is adhered to throughout the system's development or update lifecycle. MDAs should consider how their business processes can be changed to be more effective by taking advantage of the opportunities provided by increased interoperability. The approval authority and final arbiter on all questions relating to EeGIF compliance will the Governing Council or MinT with the delegation of the task from the Governing Council. In this regard, MInT will

endure the responsibility of providing guidance to the requesting MDAs. The Governing Council will monitor compliance through the various Interoperability Working Groups to be established under the council.

5.3 Compliance Level and Procedure

Compliance, towards the execution phase, requires establishing and evidence that the organization as well as the particular project are operating in accordance with the set standards and principles of the EeGIF. Thus, the compliance can be done at both MDA or project level. While the MDA level compliance ensures that the particular MDA capacity is in line with the expectation of organizational compliance, the project level compliance will confirm whether the particular project is in conformity with the standards and procedures of the EeGIF and related requirements. The detailed description of these levels of compliance and a high-level activity diagram showing the compliance process is presented in the upcoming sections.

5.3.1 Organizational Compliance

For organizational level compliance, the MDA is expected to demonstrate that it has the capability and the required infrastructure that enables it to initiate, plan, execute and run information systems projects. The organizational compliance should be done in a yearly basis where MDAs present the required documentation as a proof of concept to demonstrate that institutional compliance is achieved.

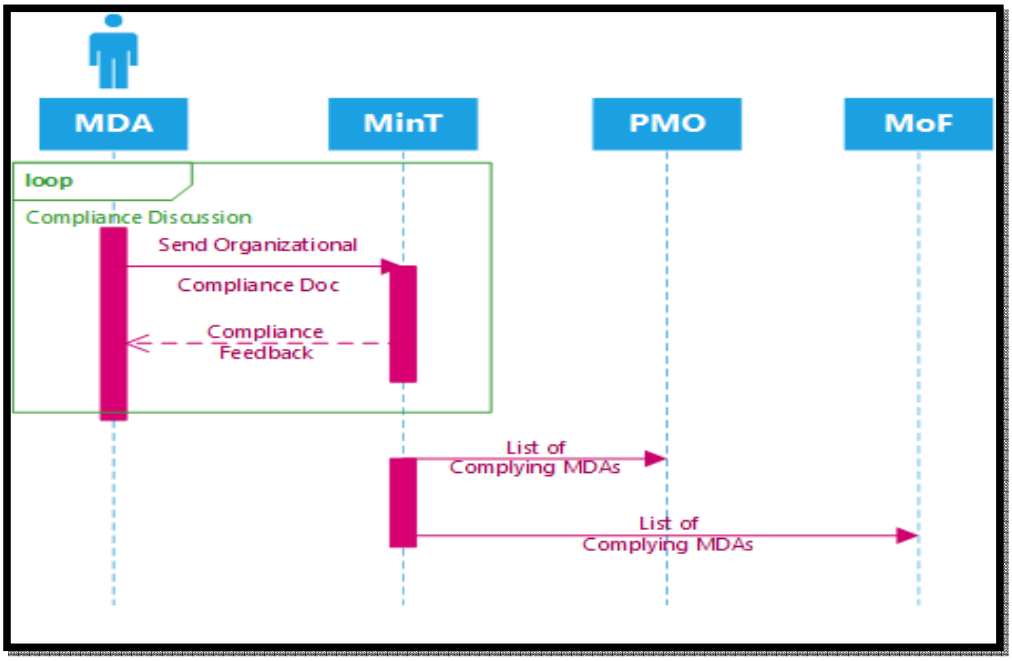


Figure 4: Organizational Compliance Activity Diagram

As shown in Figure 4, MDAs are required to present and demonstrate their compliance with the EeGIF requirements where there might be a back-and-forth between MinT (if tasked by the GC) to get compliance certificate. The decision of compliance, after the final decision, shall be sent both to Ministry of Finance and the PMO who are releasing project funds and oversee the interoperability respectively. The organizational compliance shall be used in the process of approving and releasing fund for new projects to be implemented at the particular MDA.

5.3.2 Project Compliance

Information system projects are initiatives that will be highly impact with the requirement of meeting the national standards. Thus, EeGIF compliance will become an integral part of project funding reviews to ensure only projects that comply with the EeGIF standards and requirements are sanctioned to proceed. Accordingly, the following project compliance confirmation activity diagram (Figure 5) is proposed which uses the organizational compliance as one of the requisites to approve and release budget.

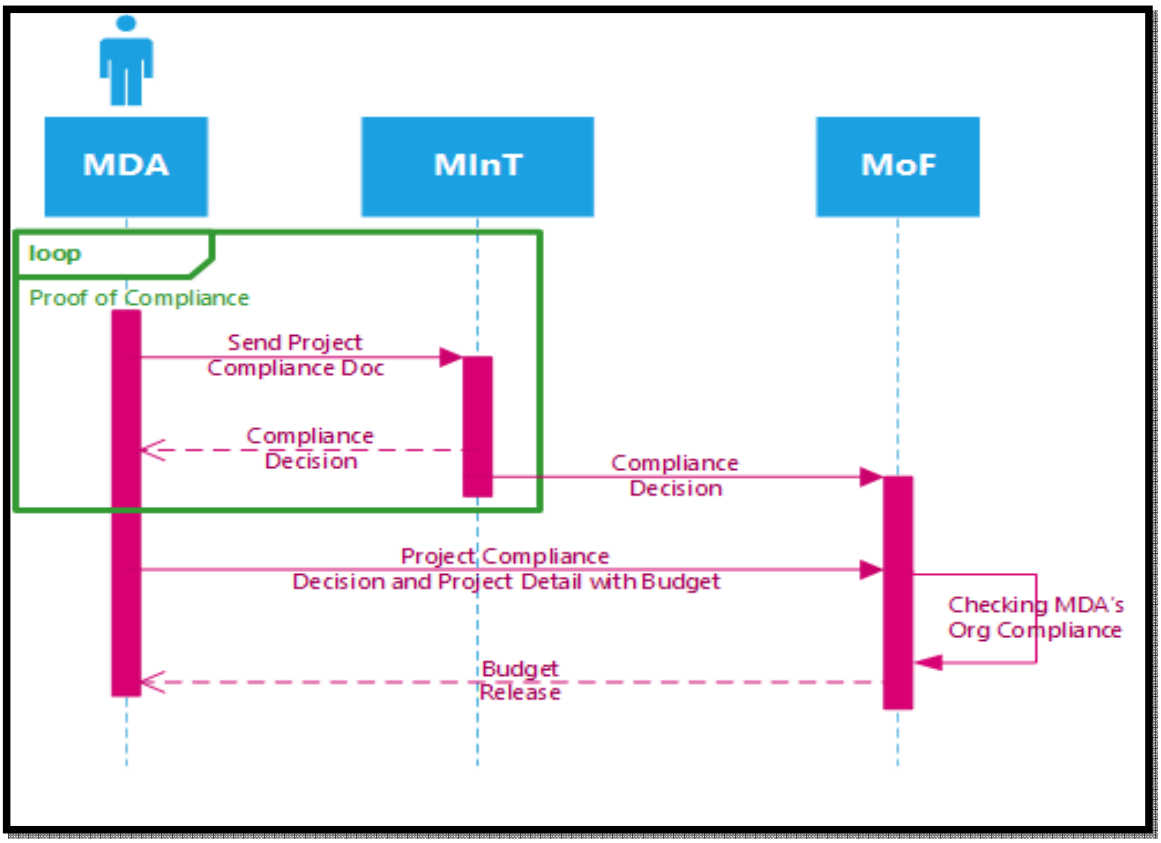


Figure 5: Project Level Compliance Activity Diagram

Similar with the organizational compliance, Figure 5 shows how MDAs should go about getting approval on project with respect to its compliance to the required EeGIF requirements. In addition to checking the compliance of the proposed project with the EeGIF requirements, the process demands an already existing organizational compliance presented to the governing council, MinT and Ministry of Finance to approve projects.

5.4 Consequences of Non-Compliance

One way of enforcing the use of Ethiopian eGovernment Interoperability Framework is a mechanism to show the consequence of non-compliance. The e-Governance systems that are, as whole or in part, non-compliant with EeGIF are subject to the following restrictions:

- ✓ Systems seeking to interface with any government database or information source, the government gateway or any governmental knowledge network (like NDC, WoredaNet, SchoolNet, any of the available Government e-Services) and failing to comply with the e-GIF may be refused connection;

- ✓ New system initiatives from MDAs failing to comply with the eGIF might not get project approval or funding from the appropriate bodies or authorities;
- ✓ Vendors and services providers who are not able to meet the compliance requirements might be excluded from competitive bids;

6 Reference

1. United Nations Development Program, Governance for sustainable human development, UNDP policy document, New York, 1997.
2. European Public Administration Network eGovernment Working Group (2004). Key Principles of an Interoperability Architecture. http://www.reach.ie/misc/docs/PrinciplesofInteroperability.pdf

7 Annex

Annex A: Interoperability Compliance Checklist

Adopting the framework

A. Individual MDA should undertake the following activities to build capability:

1. Existence of assigned responsibility for information management and Information Interoperability to senior executives.
2. Established governance arrangements with agencies in the same sector to develop plans, standards, and practices for improving information exchange across the sector.
3. Use of tools to facilitate effective information sharing across agencies.
4. Assess agency information-management capability.
5. Comply with agreed standards used across government as per the Technical Standard.
6. Implement regular formal reporting to senior managers/Ministers on progress towards achieving Information Interoperability.
7. Providing specific and continuous training to officers and experts at all levels

Enabling Information Interoperability as part of the information lifecycle

A. To address interoperability through a life-cycle approach MDAs should:

1. Identify the potential uses of new information collections, particularly any potential for use by other agencies and citizens and any long-term storage requirements, and address these uses in the planning and designing stage.
2. Adopt standard data item concepts and definitions so that information can be easily compared.
3. Consider any potential barriers to making the information available to others, such as third-party license and restrictions.

B. Prior to creating new information holdings MDAs should:

1. Undertake a review to determine if the information required can be sourced from an existing collection.

C. In collecting information MDAs should:

1. Inform the providers of the information of the purpose and intended uses of the collection and seek appropriate consents.
2. Monitor and manage the quality of information as it is collected to ensure that it is accurate and adequately meets the intended purpose.

D. To better support users, MDAs should:

1. Organize and store information in a manner where common requests for access can be serviced efficiently.
2. Organize and store appropriate metadata, so that information can be described to users easily and efficiently.

E. MDAs should adopt the following practices to facilitate appropriate access to information holdings:

1. Make information holdings and data collections visible in relevant networks, portals and directories.
2. Consider whether special access protocols are required to allow appropriate access to sensitive information.
3. Document and publish access and use conditions that will apply to the information and provide a contact point for information requests.
4. Ensure that privacy, confidentiality and security as well as other legislated obligations are met when servicing information request.
5. Meet requests in a timely and efficient manner.

F. In facilitating the use of information holdings, MDAs should:

1. Consider whether there is a need to provide special support and education to key users.
2. Consider establishing supply-use agreements and Information Sharing Protocols with key users to provide certainty and clarity around service levels, conditions and responsibilities.

G. The information lifecycle includes the effective maintenance of information, and in some circumstances, its disposal. With this is mind, MDAs should:

1. Liaise with users when considering ceasing, disposing of, or making content changes to collections.
2. Conduct audits and reviews of security, quality, accessibility and compliance with access and use conditions.

Partnerships and Collaboration

A. To promote partnerships and collaborations, agencies should:

1. Identify other agencies they need to share information with and consider forming a partnership to manage information exchanges and the joint development of Information Interoperability capability.
2. Develop plans and agreements with other agencies for information management and exchange.
3. Promote awareness of the Ethiopia Government information management principles and the benefits of Information Interoperability.
4. Foster a culture of trust and collaboration with partner agencies.
5. Educate officers on the business drivers, policy and legal obligations of partner agencies.
6. Ensure that information management and exchange initiatives are adequately funded.
7. Monitor progress and review outcomes.

Authoritative Sources of Information

A. To develop and support authoritative sources, agencies should:

1. Identify other potential users and uses of their information holdings and design and manage their information in the context of appropriate and agreed uses.
2. Consider entering into formal information supply/exchange agreements with other agencies to support effective utilization of authoritative information sources.
3. Promote accessibility of authoritative information sources by adopting the Technical

Interoperability Framework Standards and constructing information systems so that information can be easily, reliably and securely supplied to other users.
4. Establish and maintain effective relationships with users of the information they hold.
5. Promote visibility and appropriate use of authoritative information holdings by publishing to relevant directories and by creating quality documentation.

Adopt common business language and standards

A. To adopt common business language and standards, MDAs should:

1. Consider whether new information standards are applicable to their holdings.
2. Seek whole-of-government development of standards where they do not exist.
3. Identify and adopt appropriate existing standards wherever possible.
4. Establish data and information management policies and processes that encourage compliance with standards.
5. Participate in relevant standard setting forums.

Establish appropriate governance arrangements

A. To establish appropriate governance arrangements, MDAs should:

1. Assign responsibility for Information Interoperability to a senior executive.
2. Ensure that appropriate governance arrangements are in place within the agency to guide policy and practice in relation to information management and interoperability.
3. Consider the need for cross-agency governance arrangements to support information exchange.
4. Establish appropriate policy on information management and exchange.
5. Conduct appropriate audits and reviews.

Facilitate an understanding of the legal and policy framework

A. To facilitate an understanding of the legal and policy framework, MDAs should:

1. Identify legislation and policy which impacts on the provision and use of their information holdings and use an information access protocol to ensure that external use of information complies with legal and policy obligations.
2. Educate staff involved in information exchange on legal and policy obligations.
3. Document and publish information access and use conditions.
4. Educate information users on their legal obligations and information use restrictions.
5. Conduct audits and reviews of compliance with access and use conditions.

Ethiopian National Enterprise Archiecture Framework (ENEAF) & E-Governement Interoperability Framework for Ethiopia (EeGIF)

Technical Standards

November 2019

Minstry of Inovation and Technology, Addis Ababa, Ethiopa

Submitted by : School of Information Science (SIS), AAU

Document:	Technical Standards Report on EEAF & E-eGIF Update version
Version:	(Update) Version 2.0
Activities:	Technical Standards
Client:	MInT
Consultant:	AAU
Experts:	Workshet Lamenew (PhD) Ermias Abebe Mesfin Kifle (PhD) Wondwoson Mulugeta (PhD) Tibebe Beshah (PhD)
Date:	November 2019

TABLE OF CONTENTS

List of Tables

Abbreviations

Abbreviation	Expansion
ASCII	American Standard Code for Information Interchange
ANSI	American National Standards Institute
BPMN	Business Process Modeling Notation
COM	Component Object Model
CSS	Cascading Style Sheet
CSV	Comma Separated Values
DES	Data Encryption Algorithm
3DES	Triple Data Encryption Algorithm
DHCP	Dynamic Host Configuration Host protocol
DNS	Domain Name Services
EA	Enterprise Architecture
ebXML	E-business XML
EDI	Electronic Data Interchange
eGIF	e-Government Interoperability Framework
EeGIF	Ethiopian e-Government Interoperability Framework
EGoT	Ethiopian Government Thesaurus
ESA	Ethiopian Standards Agency
FTP	File Transfer Protocol
FTPS	Secure File Transfer Protocol
GIF	Graphics Interchange Format
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
ICT	Information and Communication Technology
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
INSA	Information Network Security Agency
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPsec	IP Security Authentication Header
ISO	International Standards Organisation

ITIL	Information Technology Infrastructure Library
JPEG	Joint Photographic Experts Group
LDAP	Lightweight Directory Access Protocol
L2TP	Layer 2 Tunneling Protocol
MIME	Multipurpose Internet Mail Extensions
MIX	Metadata for Images in XML
MP-BGP	Multi Protocol-Border Gateway Protocol
MPEG	Moving Picture Experts Group
MSAG	Multi Service Access Gateway
MSDP	Multi Source Discovery Protocol
MTA	Message Transfer Agent
NALA	National Archives & Library Agency
OASIS	Organization for the Advancement of Structured Information Standards
OS	Operating System
PDF	Portable Document Format
POP	Post Office Protocol
POSIX	Portable Operating System Interface
PPP	Point to Point Protocol
PKI	Public Key Infrastructure
QoS	Quality of Service
RDF	Resource Description Framework
RMON	Remote Network Monitoring
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SVG	Scalable Vector Graphics
S/MIME	Secure/Multipurpose Internet Mail Extensions
TCP	Transmission Control Protocol
TIFF	Tagged Image File Format
UDDI	Universal Description Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling language
VPN	Virtual Private Network
WCAG	Web Content Access Guidelines
WML	Wireless Markup Language

WSDL	Web Service Definition Language
WSS	Web Services Security
WS-I	Web Services-Interoperability
W3C	World Wide Web Consortium
XHTML	Extensible Hypertext Markup Language
XMPP	Extensible Messaging and Presence Protocol
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XNAL	Extensible Name and Address Language
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformation

1 Background

The government administration in Ethiopia is a multi-tier organization, having departments at national, regional and woreda levels at each region. Government's initiative to enable citizen services across the country using IT enabled resources is huge and complex. With the diversity of people, cultures, incomes, backgrounds and with different levels of expectations across different demographics, this task becomes even more complex. Unless there are standards and well-defined guidelines, this complexity can lead to confusion and may not provide the desired objective.

Unless the entire approach is carried out in a structured approach, things can become too complex to handle. An Enterprise Architecture Framework (EAF) would guide these initiatives in a desired manner and enable the government to realize its vision by finding the right balance, the right level of interaction, the right governance models, and other attributes at the national level.

Standards form one of the key components of the National Enterprise Architecture Framework for Ethiopia (ENEAF.) Sstandards in ENEAF are chosen from internationally available and accessible standards which are widely in use. Since EA Framework is aimed to facilitate the ability of government organisations to share information and to integrate information and business processes it is essential to agree to use common standards.

Standards are defined for different aspects of an EA and there are various ways of classifying them. Countries adapt may adapt classifications depends on their situation and international practices. The classification of standards usually depends on the level of maturity of the countries implementing the EA. In consequence, each country may call the standard areas in different names.

Moreover, as per the principles defined for ENEAF, it is strongly recommended to adopt open standards. As TOGAF has been recommended as the base framework for Ethiopia, the technical standards proposed in this document are guided by the core architectures: Business, Data, Application and Technology.

As discussed in the ENEAF and governance document of Ethiopian Electronic Government Interoperability Framework (EeGIF), interoperability is a core pillar to facilitate EA implementation.

This document, then after referred as Technical Standards, is defined the baseline technical standards for ENEAF and EeGIF. It is organized into two sections. The first section gives highlight on dimensions in relation to standards, scope of this document, the standards coverage, and finally the update process put in place. The second section covers details of the technical standards which are classified into nine technical areas: Business Architecture and Modeling, Application, Enterprise IT Management, Platforms, Interconnection, Data Exchange, Security, Metadata and Data Standards, and Access/Discovery.

1.1 Dimensions

At the top level, standards are classified in line with the TOGAF architecture domains, including the following areas:

- **Business Standards**:
  - Standard for business modelling
  - Security and governance standards for business activity
- **Data Standards:**
  - Standard coding and values for data
  - Standard structures and formats for data
  - Standards for data exchanges
- **Applications Standards:**
  - Standards for application communication and interoperation
  - Standards for access, presentation, and style
  - Standards for applications development
- **Technology Standards;**
  - Standard for hardware products
  - Standard for software products

In the otherside, interoperability aspects are covered in the various dimensions of interoperability standards that are adopted globally, namely:

- Organizational interoperability;
- Information or semantic interoperability; and
- Technical interoperability.

These dimensions are also the capabilities of eGIF. These capabilities are required to improve the interoperability. The improvement is achieved through the right mix of policy, structure, standards, process, mangement and technology across all capabilities (organisation, semantic, and technology).

Organizational Interoperability:

It is concerned with collaboration between entities in the development, deployment and delivery of e-Government services, and to the interaction between services, and supporting processes. Specifically, business process or organizational interoperability deals with defining organisation goals, common methods, modeling business processes, defining shared services etc. This is particularly critical to facilitate ease-of-doing-business through eService applications. Neverthless, it is a very sensitive and challanging task and requires high level of authroithy at national level and streamline all concerned units. In this document, only modeling related standards are proposed. Business process or electronic service level interoperability standards shall work out by the structure described in the governence document.

Information or semantic interoperability:

Semantic interoperability is concerned with the communities of practice and to the negotiation of meaning that occurs within them. It is also concerned with ensuring that the exact meaning of information from various applications are understandable by any application even though if the application was not developed for this purpose'. For e.g. semantic interoperability services can be used when a citizen relocates his home and business from one city to another by means of a single interaction. Linking the user's name to their business and retrieving residential and business addresses, telephone numbers etc. will ensure interoperability. In some countries they prepare a common words thesaurus for commonly used terms, for example in accounting and administration functions all ministries and agencies make use of terms such as Acquisitions, Contracting out, e-Procurement, Outsourcing, Procurement and Tendering. These terms are defined clearly and standard connotations are provided. The effort is in first identifying the area, then defining the semantics and lastly institutionalising the usage. Interoperability at this level can fail if different users, or groups of users, use different terms for similar concepts, or use similar terms to mean different things. In this document, minimum baseline standards are recommended by referring to the Dublin Core

recommendations on metadata standard. The need of Ethiopian Government Thesaurus (EGoT) is suggested as its importance is underlined in other official doucments of MInT. Further detail standards shall be worked out when the ENEAF & EeGIF governance be in placed.

Technical Interoperability:

Technical interoperability is the most common and basic aspect of interoperability. This is necessary to ensure that all the hardware and software components of the network and information system can physically communicate and transfer information successfully. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services etc. The interaction among elements that correspond to various technological waves, particularly relevant in relation to preservation and access of information on the electronic media need to be considered in technical interoperability. In this document, a couple of technical standards are proposed.

1.2 Scope:

There are 9 technical standards areas covered under this document - namely Business Architecture and Modeling, Application, Enterprise IT Management, Platforms, Interconnection, Data Exchange, Security, Metadata and Data Standards, and Access/Discovery. The 9 areas were identified based on the:

- The areas presented in the previous ENEAF (v5.0) and EeGIF (V1.0)
- Best practice review to get an idea of the leading practice industry standards
- Understanding of maturity level and transformational values of existing and emerging technologies through technology trends.
- Information on the Ethiopian Standards Organization (ESA) standards catalogue, Information and Network Security Agency (INSA) standards, etc
- Information on International Standards organisation such as IETF, W3C, ISO/IEC, OASIS, Dublin core, etc.

2 NEEAF & EeGIF Standards

In NEEAF and EeGIF, many standards are adopted as necessary. Use of these standards will bring Leading Practices, Interoperability, reuse and collaboration to bear upon e-Governance efforts to develop and deploy services.

These standards are chosen from internationally available and accessible standards which are widely in use. ICT Products are designed and developed in conformity with the standards. Since NEEAF and EeGIF is aimed to facilitate the ability of government organisations to share information and to integrate information and business processes it is quintessential to agree to use common standards. It should be noted that these standards evolve as innovations drive new technologies, products and improvements to existing products.

There must be a mandatory compliance with the accepted standard, interface and architecture at all levels to be interoperable, so that data and information can be exchanged and processed seamlessly across government.

The proposed standards are presented in a tabular structure for each technical area. The standards table will have many 'Components'. Each component will have:

- the standards name,
- title and version,
- enforcement category as Mandatory or Recommendatory,
- for additional information on each component/standard, the details of the standards with resource locator (source) to the relevant standard is provided, and
- the name of the standard body.

The brief overview of the nine technical areas and the respective components are presented in Table 2-1 followed by the standards table.

Table 2-1: Technical Areas

Technical Areas	Components
Business Architecture and Modeling	• Business Process Modeling • Business Archiecture Modeling

Application	• Modeling, Design and Development
Enterprise IT Management	• IT Service Management • Management Protocols • Monitoring & Protocol Access
Platforms	• Desktop Operating System • Hardware Platform
Interconnection	• Application Layer Protocols • Transport Layer Protocols • Link Layer Protocols
Data Exchange	• Character and encoding for information interchange • Data description, Data exchange & Transformation • Data Formats • Digitization • Data Definition for Smart Cards
Security	• Digital Signature • Email Security • Encryption Algorithm • Web Service and XML Security • Identity , Authentication , authorization and privacy • Network Level Security • Wireless LAN Security • Remote Security • Secure transport • Others
Metadata and Data Standards	• Ethiopian Government Thesaurus (EGoT) • Metadata Core • Metadata • Data Standards • Metadata Technologies/standards • Metadata Registry
Access/Discovery	• Discovery • Smart Card • Web Access standard

2.1 Business Architecture and Modelling

This section provides a list of the relevant standards in business architecture and modeling along with links for references to these standards

Table 2-2: Business Architecture and Modeling

Business Architecture and Modeling			
Standard	**Title / Specification (Version/URL)**	**Mandatory/ Recommendatory**	**Standards Body**
BUSINESS PROCESS MODELLING			
BPMN	Business Process Modelling Notation version 2.0 http://www.omg.org/spec/BPMN/2.0/	Recommendatory	OMG
WS-BPEL (BPEL)	Business Process Execution Language http://www.oasisopen.org/committees/wsbpel	Recommendatory	OASIS
BUSINESS ARCHITECTURE MODELLING			
TOGAF	The Open Group Architecture Framework version 9.3 https://www.opengroup.org	Recommendatory	The Open Group

2.2 Application

This section provides a list of the relevant standards in application area along with links for references to these standards.

Table 2-3: Application

Application			
Standard	**Title / Specification (Version/URL)**	**Mandatory/ Recommendatory**	**Standards Body**
MODELLING, DESIGN AND DEVELOPMENT			
UML	Unified Modeling Language; version 2.5 https://www.omg.org/spec/UML/2.5/	Recommendatory	OMG

2.3 Enterprise IT Management

This section provides a list of the relevant standards in Enterprise IT Management along with links for references to these standards.

Table 2-4: Enterprise IT Management

Enterprise IT Management			
Standard	**Title / Specification (Version/URL)**	**Mandatory/ Recommendatory**	**Standards Body**
IT SERVICE MANAGEMENT			
ITIL	Information Technology Infrastructure Library Version 3.0 https://www.itlibrary.org	Recommendatory	OGC (UK Government's Office

			of Government Commerce
MANAGEMENT PROTOCOLS			
SNMP	Simple Network Management Protocol; version 3 http://tools.ietf.org/html/rfc1157 http://tools.ietf.org/html/rfc3411	Mandatory	IETF
MONITORING AND PROTOCOL ACCESS			
RMON	Remote Network MONitoring version 2.0 http://tools.ietf.org/html/rfc2819 http://tools.ietf.org/html/rfc3577	Mandatory	IETF

2.4 Platforms

This section provides a list of the relevant standards in platforms along with links for references to these standards.

Table 2-5: Platforms

Platform			
Standard	**Title / Specification (Version/URL)**	**Enforcement Category: Mandatory/ Recommendatory**	**Standards Body**
Desktop Operating Systems			
POSIX	Portable Operating System Interface http://standards.ieee.org/regauth/posix/	Mandatory	IEEE
HARDWARE PLATFORMS			
x86	Instruction set architecture (x86-32/x86-64)	Recommendatory	

2.5 Interconnection

This section provides a list of the relevant standards in interconnection along with links for references to these standards.

Table 2-6: Interconnection

Interconnection			
Standard	**Title / Description (Version/URL)**	**Enforcement Category: Mandatory/ Recommendatory**	**Standards Body**
Application Layer Protocols			
DNS	Domain Name Service	Mandatory	
FTP	File Transfer Protocol; RFC 765 http://www.ietf.org/ rfc/rfc765.txt, rfc114.txt	Mandatory	**IETF**
SFTP	Secured File Transfer Protocol http://www.ietf.org/ rfc/rfc765.txt, rfc114.txt	Mandatory	**IETF**
HTTP	Hypertext Transfer Protocol	Mandatory	**IETF**
HTTP2	Hypertext Transfer Protocol – HTTP 2; RFC 7540 https://tools.ietf.org/html/rf7540	Mandatory	**IETF**
HTTPS:TLS	Transport Layer Security Protocol Version 1.2	Mandatory	**IETF**

	RFC 5246 https://tools.ietf.org/html/rfc5246		
LDAP	Light Weight Directory Access Protocol	Mandatory	
MIME	Multipurpose Internet Mail Extensions; RFC 2045, 2046,2047, 2049,4289 & 6838 https://tools.ietf.org/html/rfc2045 https://tools.ietf.org/html/rfc2046 https://tools.ietf.org/html/rfc2047 https://tools.ietf.org/html/rfc2049 https://tools.ietf.org/html/rfc4289 https://tools.ietf.org/html/rfc6838	Mandatory	**IETF**
SNMP	Simple Network Management Protocol	Mandatory	
SOAP	Simple Object Access Protocol, v1.2 https://www.w3.org/TR/2001/WD-soap12-20010709/	Mandatory	**W3C**
SSH	The Secure Shell Protocol RFC 4250 to 4254 https://tools.ietf.org/html/rfc4250 https://tools.ietf.org/html/rfc4251 https://tools.ietf.org/html/rfc4252 https://tools.ietf.org/html/rfc4253 https://tools.ietf.org/html/rfc4254	Mandatory	**IETF**
Transport Layer Protocols			
TCP	Transmission Control Protocol RFC 793 https://tools.ietf.org/html/rfc793	Mandatory	**IETF**
UDP	User Datagram Protocol; RFC 768 http://www.ietf.org/ rfc/rfc768.txt	Mandatory	**IETF**
Others			
ESA Standards	35.110: NETWORKING http://www.esa.gov.et/ethiopian-standards	Recommedatory	ESA

2.6 Data Exchange

Data Integration provides for aggregation of data from disparate sources and facilitates inter organisational communication. Use of standards for representation of data and suitable converters such as Optical Character Recognizing (OCR) engines enable aggregation. It covers components and technical specifications required to support the recognition of data (txt, images, maps and multimedia.), codes, recognition methods, interpretation formats, converters and filters.

Table 2-7: Data Exchange

Data Exchange			
Standard	**Title / Specification (Version/URL)**	**Enforcement Category: Mandatory/ Recommendatory**	**Standards Body**
Character and encoding for information interchange			
UNICODE	set of standards for character encoding http://www.unicode.org/versions/latest/	Mandatory	Unicode Technical Committee

Data Description, Exchange and Transformation			
XSD	XML Schema Definition Language https://www.w3.org/TR/xmlschema11-1/	Mandatory	W3C
XML 1.0	Extensible Markup Language 1.0 Fifth Edition; https://www.w3.org/TR/xmldsig-core/	Mandatory	**W3C**
XMI 2.0.1	XML Metadata Interchange; version 2.0.1; ISO/IEC 19503; http://www.omg.org/spec/XMI/	Mandatory	**ISO/IEC**
XSL v1.1	Extensible Stylesheet Language version 1.0; https://www.w3.org/TR/xslt	Mandatory	**W3C**
XSLT v2.0	XSL Transformations version 3.0; https://www.w3.org/TR/xslt20/	Mandatory	**W3C**
Xpath 2.0	XML Path Language (XPath) http://www.w3.org/TR/xpath20/	Recommendatory	W3C
GML	Geography Markup Language Version 3.3 http://www.opengeospatial.org/standards/gml	Recommendatory	Open Geospatial Consortium
ebXML v2.0	ebXML Message Service Specification v2.0 200204/ http://docs.oasisopen.org/ebxmlbp/2.0.4/OS/spec/ebxmlbpv2.0.4-Spec-os-enhtml/ebxmlbp-v2.0.4-Specos-en.htm	Recommendatory	OASIS
ebMXL v3.0	ebXML Messaging Services Version 3.0 http://docs.oasisopen.org/ebxmlmsg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html	Recommendatory	OASIS
Data Formats			
PDF	Portable Document Format version 1.7; ISO 32000-1 http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf	Mandatory	**ISO**
PDF/A	Document management – Electronic document file format for long term preservation; version 1.7; - ISO 19005-2 PDF 1.7 (ISO 32000-1:2008) -2011 - ISO 19005-3 PDF 1.7 (ISO 32000-1:2008) –2012 http://www.digitalpreservation.gov/formats/fdd/fdd000318.shtml	Recommendatory	**ISO**
PNG	Portable Network Graphics Specification Version 1.0; https://www.w3.org/TR/REC-png-multi.html	Mandatory	**W3C**
SVG 1.1	Scalable Vector Graphics version 1.1; https://www.w3.org/TR/SVG/	Recommendatory	**W3C**
TIFF	Tagged Image File Format version 6.0; https://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf	Mandatory	**Adobe Systems**
GIF	Graphic Interchange Format; http://giflib.sourceforge.net/	Recommendatory	**Compuserve**
JPEG	Joint Photographic Experts Group; ISO/IEC 10918; http://www.iso.org/iso/catalogue_detail.htm?csnumber=18902	Recommendatory	Joint Photographic Experts Group
MPEG-1	Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s ISO/ IEC 11172:1993 http://www.iso.org/iso/catalogue_detail.htm?csnumber=22412	Recommendatory	**ISO/IEC**

MPEG-2	Generic coding of moving pictures and associated audio information ISO/IEC 13818-1: 2015 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67331	Recommendatory	**ISO/IEC**
MPEG-4	Coding of audiovisual objects ISO/ IEC 14496:1998 http://mpeg.chiariglione.org/	Recommendatory	**ISO/IEC**
MPEG-7	Multimedia content description interface; ISO/ IEC 15938:2002 http://www.iso.org/iso/catalogue_detail.htm?csnumber=34229	Recommendatory	**ISO/IEC**
MPEG-21	Multimedia framework ISO/ IEC 21000:2001 http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=40611	Recommendatory	**ISO/IEC**
HTML	Hypertext Markup Language; Version 5.0; https://www.w3.org/TR/html4/	Mandatory	**W3C**
XHTML	Extensible Hypertext Markup Language Version 1.1.1 https://www.w3.org/TR/xhtml1/	Mandatory	**W3C**
HTML5	Hypertext Markup Language 5: A vocabulary and associated APIs for HTML and XHTML standard https://www.w3.org/TR/html5/	Mandatory	W3C
CSS	Cascading Style Sheets, level 1 CSS 2.2 https://www.w3.org/TR/CSS22/	Mandatory	**W3C**
DOM	Document Object Model Level 2 Style Specification https://www.w3.org/TR/DOM-Level-2-Style/	Mandatory	**W3C**
OOXML	Office Open XML File Formats – ISO/ IEC 29500-1: 2012 http://www.iso.org/iso/catalogue_detail.htm?csnumber=61750	Mandatory	**ISO/IEC**
ODF	Open Document Format for Office Applications version 1.1 & 1.2; http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485 https://www.oasisopen.org/committees/office	• Recommendatory	• ISO/IEC; OASIS •
ZIP	Archive file format that supports lossless data Compression V6.3.4 https://support.pkware.com/display/PKZIP/APPNOTE	Recommendatory	PKWARE
GNU gzip	Software application for file compression and Decompression RFC 1952; https://tools.ietf.org/html/rfc1952	Recommendatory	GNU GPLv3
GNU tar	Create tar archives V1.28 https://www.gnu.org/software/tar/	Recommendatory	GNU
Others			
ESA Standards	35.140: COMPUTER GRAPHICS 35.240.30: ITs Applications In Information, Documentation And Publishing 35.240.70: IT'S APPLICATIONS IN SCIENCE http://www.esa.gov.et/ethiopian-standards	Recommendatory	ESA

2.7 Security

Security covers components and technical specifications needed to enable the secure exchange of information as well as the secure access to public sector information and services.

Table 2-8: Security

Security			
Standard	**Title / Specification (Version/URL)**	**Mandatory/ Recommendatory**	**Standards Body**
Digital Signature			
DSA	Digital Signature Algorithm; FIPS PUB 186-4; http://nvlpubs.nist.gov/nist pubs/FIPS/NIST.FIPS.186-4.pdf	Mandatory	**NIST**
SHA2	Secure Hash Algorithms; NIST FIPS PUB 180-4; http://csrc.nist.gov/publicati ons/fips/fips180-4/fips-180-4.pdf	Mandatory	**NIST**
SHA3	Secure Hash Algorithms; FIPS PUB 202; http://csrc.nist.gov/publicati ons/drafts/fips-202/fips_202_draft.pdf	Mandatory	**NIST**
Email Security			
S/MIME (ESS)	Secure/Multipurpose Internet Mail Extensions **(Enhanced Security Services); Version 3.0; RFC 5035;** https://tools.ietf.org/html/rfc5751	Mandatory	**IETF**
Encryption Algorithm			
RSA	Asymmetric public key cryptographic algorithm; IEEE 1363; http://grouper.ieee.org/groups/1363/	Recommendatory	**IEEE**
AES	Advanced Encription Standard; FIPS PUB 197; http://csrc.nist.gov/publications/fips/fips197/f ips-197.pdf	Recommendatory	**NIST**
3DES	Triple Data Encryption Standard (3DES). FIPS 46-3 and ANS X9.52-1998	Recommendatory	
Web Service and XML Security			
WS Security	Web Services Security Version 1.1.1; OASIS 20040; http://docs.oasisopen. org/wssm/wss/v1.1.1/os/wss-UsernameTokenProfilev1.1.1-os.html	Mandatory	**Organization for the Advancement of Strctured Information Standards**
WS-I Basic Security profile	Web Services Interoperability Organization – Basic Security Profile Version 1.0; http://www.wsi.org/profiles/basicsecurityp rofile-1.0.html	Manadatory	**Organization for the Advancement of Strctured Information Standards**
XML-DSIG	Extensible Markup Language- Signature Sintax and Processing; Xmldsig-core-20080610; 2nd edition; https://www.w3.org/TR/xmldsig-core	Mandatory	**W3C**

XML Encryption	XML Encryption http://www.w3.org/TR/xmlenc-core/	Recommendatory	W3C
XML Signature	XML Signature for XML Message signing; http://www.w3.org/TR/xmldsig-core/	Recommendatory	W3C
Identity , Authentication , authorization and privacy			
X.509	International Standard for identiity certificate, version 3; RFC 6818; https://tools.ietf.org/html/rfc6818	Mandatory	**IETF**
SAML	Security Assertions Mark-up Language, Version 2.0; https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=security	Mandatory	**OASIS**
Network Level security			
IPSec.	Internet Protocol Security RFC 2402/2404	Mandatory	**IETF**
IP ESP	IP Encapsulating Security Payload; RFC 2406	Recommendatory	IETF
Remote Security			
SSH.	Secure Shell Protocol; RFC 4250 – 4254; https://tools.ietf.org/html/rfc4250 https://tools.ietf.org/html/rfc4251 https://tools.ietf.org/html/rfc4252 https://tools.ietf.org/html/rfc4253 https://tools.ietf.org/html/rfc4254	Mandatory	**IETF**
Wireless LAN Security			
WPA 2.0	Wi-Fi Protected Access	Mandatory	
Secure Transport			
TLS	Transport Layer Security Protocol Version 1.2; RFC 5246; https://tools.ietf.org/html/rfc5246	Mandatory	**IETF**
SSL	Secure Socket Layer Protocol; Version 3.0; http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00	Mandatory	**IETF**
Others			
ESA Standards	ES ISO 22307-6:2012 ES ISO/TR 14742:2012 http://www.esa.gov.et/ethiopian-standards	Recommendatory	ESA
INSA Standards	Critical Mass Cyber Security Requirement Standard; Version 1.0 http://www.insa.gov.et/	Recommendatory	INSA

2.8 Meta Data and Data Standard

Meta data can be thought of as Data about other data. It is the internet-age term for what librarians traditionally have put into catalogs. It is descriptive about information resources (including web resources). It consists of a set of attributes or elements considered necessary (useful) to describe the resource in question.

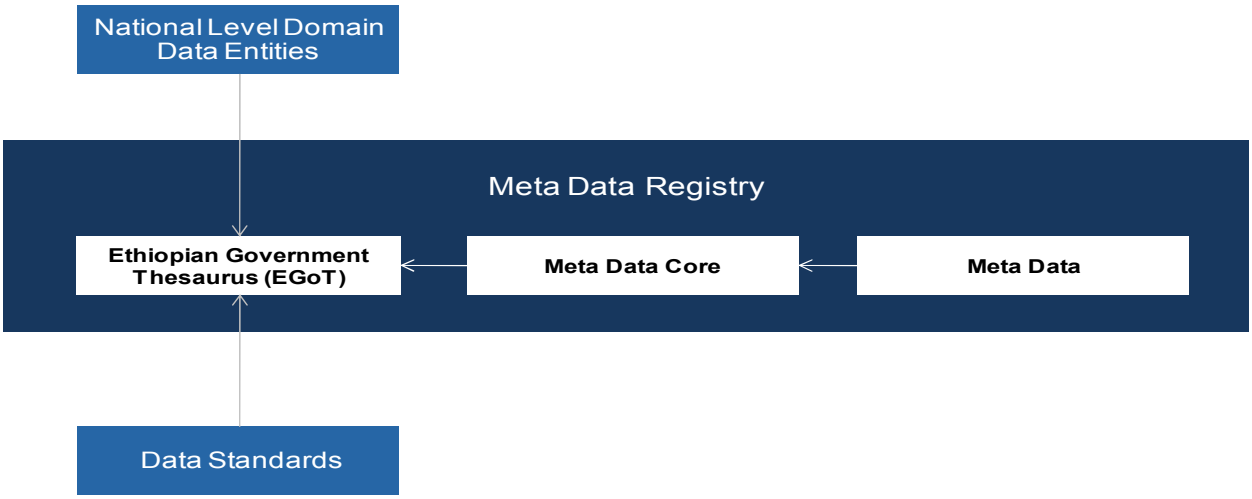


Figure 2-1: Meta Data and Data Standards

Ethiopian Government Thesaurus (EGoT)

The standards to use for these have to be developed as per a defined process which ensures coordination. EGoT – Ethiopian Government Thesaurus will provide the starting point. The Thesaurus will contain entities (data items) of use both generic (useful across ministries) and special (useful to specific ministry based on National Level Domain Entities). The data items can be gleaned from current ICT applications, planned/ in progress ICT applications and future ICT applications (e-Services). The Thesaurus will have structure reflecting the generic and the special segment. The Thesaurus will have to be updated as per an established process with maintenance tools. Few examples of entities are Address, Persona name etc.

Data Standards

For each entity/group of entities in EGOT, description of details/structure of the entity (with attributes) is provided in Data Standards. The detail may also include as appropriate high level digital representation for access and use. Examples of Data standard are for entity Company Registration number, Name, Head office, Tel. Number, Type of company, Year of registration.

Meta Data Core

These are core set of Metadata, that may be described using XML. To publish and make available and facilitate access, metadata about data standards as per Dublin core with elements and qualifiers is Recommendatory for use. These Metadata will be used for every and any type of document.

Meta Data

These will comprise attributes about data additional to the Dublin core in accordance with the elements and qualifiers of the Dublin core e.g. in library management, Contact, document form, citation, channels etc. These Metadata can be domain specific which will get reflected on any document including data standards.

National level Domain Data Entities

This envision creation and maintenance of national level data domain entities in accordance with a coordinated process. These data entities will establish and keep upto date the EGoT. The entities are domain specific e.g. Agriculture, Health, Education, Transport etc.

Meta Data Registry

The Meta data core, Meta Data and EGoT will be held in a Registry (Meta Data Registry) which may be conceptually understood as a catalogue in a Library of books. By using tools the registry can be searched for selection and retrieval in application development thus enabling reuse. Adding resources to the Registry enables collaboration. There are tools to manage the master data that is stored in the database and keep it synchronized with the transactional systems.

The meta data standards given in this EeGIF version 1.0 is a structure with details on Meta data core, sample meta data, sample data standards structure and initial set of Government Thesaurus with common entities. The following should be entrusted to the Meta data working group

- Endorsement of Elements of Dublin core and its adoption
- Develop a Ethiopian Government Thesaurus (EGoT)
- Define national Level Domain entities (ministry wise or common)
- Define Data Standards, and
- Develop a registry.

Metadata Technologies/Standards

Metadata technologies/standards are technologies, specification and tools that are used to create, maintain and manage Metadata Framework.

Table 2-9: Meta Data and Data Standard

Meta Data			
Standard	**Title / Specification (Version/URL)**	**Mandatory/ Recommendatory**	**Standards Body**
Dublin Core Metadata Element set	ISO15836:2009 http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=52142http://dublincore.org/	Recommendatory	ISO/IEC; DCMI

•			
Ethiopian Government Thesaurus (EGoT)			
	To-be Developed by the Governing Council		
Meta Data Core			
Meta data core based on Dublin standards	Title Creator/Author Subject and Keywords Description Publisher Contributor Date Resource Type Format Resource Identifier Source Language Relation Coverage Rights Management Accessibility Addressee Aggregation Audience Digital signature Disposal Location Mandate Preservation Status	Mandatory	Dublin Core
Meta Data			
Dataset Metadata	structure of a Dataset	Mandatory	Ethiopian National Data Set
Data Element Metadata Definition	Data Elements within a Dataset; sets rules used for Machine Reading and serving of Datasets	Mandatory	Ethiopian National Data Set
Data Source Metadata Definition	describes the source for each dataset	Mandatory	Ethiopian National Data Set
Organization Reference Metadata	describes the Organizational Stakeholders for each Dataset.	Mandatory	Ethiopian National Data Set
Data Standards			
	To-be developed by the Governing Council		
Meta Data Technologies/Standards			

XrML	Extensible Rights Markup Language Version 2.0 http://www.xrml.org/	Recommendatory	ContentGuard
MIX 2.0	NISO Metadata for Images in SML MIX Schema v2.0 http://www.loc.gov/standards/mix/	Recommendatory	Library of Congress
OAI-PMH	Open Archives Initiative Version 2.0 https://www.openarchives.org/OAI/openarchivesprotoc	Recommendatory	Open Archives Initiative
ODRL 1.1	Open Digital Rights Language Version 2.1 https://www.w3.org/community/odrl/	Recommendatory	IPR Systems
Meta Data Registry			
ISO/IEC 11179	Information Technology –Metadata Registries –Framework 11179-1 3rd edition http://metadatastandards.org/11179/	Recommendatory	ISO/IEC

2.9 Access/Discovery

Access relates to provision to be made to enable users to effectively access information and service electronically via a range of delivery channels (e.g. World Wide Web) and devices (e.g. personal computers, mobile phones, Tablets) for their needs via a range of delivery channels. This is realized by using components as per technical specifications standards to enable delivery of service, user interfaces and interaction models.

Table 2-10: Access/Discovery

Access			
Standard	**Title / Specification (Version/URL)**	**Enforcement Category: Mandatory/Recommendatory**	**Standards Body**
Discovery			
DNS	Domain Names –Concepts and Facilities, Domain Names – Implementation and Specification; RFC 1034, 1035 https://tools.ietf.org/html/rfc1034 https://tools.ietf.org/html/rfc1035	Mandatory	**IETF**
IPv4	Internet Protocol: DARPA Internet Program Protocol Specification RFC 791 https://tools.ietf.org/html/rfc791	Mandatory	**IETF**
IPv6	Internet Protocol, Version 6 Specification; RFC 2460 https://tools.ietf.org/html/rfc2460	Mandatory	**IETF**
SMTP	Simple Mail Transfer Protocol; RFC 5321 https://tools.ietf.org/html/rfc5321	Mandatory	**IETF**
IMAP4	Internet Message Access Protocol 4; RFC 3501 https://tools.ietf.org/html/rfc3501	Mandatory	**IETF**
LDAP	Lightweight Directory Access Protocol (LDAP): Technical Specification RoadMap RFC 4510 https://tools.ietf.org/html/rfc4510	Mandatory	**IETF**
IEEE 802.1	wireless connectivity to automatic machinery, equipment http://standards.ieee.org/findstds/standard/802.11n-2009.html http://standards.ieee.org/getieee802/download/802.11n-2009.pdf	Mandatory	**IEEE**
Dublin Core Standard	Simple and extensible metadata element set intended to facilitate discovery of electronic resources http://dublincore.org	Recommendatory	Dublin Core Metadata Initiative
WSDL v2.0	Web Services Description Language (WSDL) Version 2.0 https://www.w3.org/TR/wsdl	Mandatory	W3C
WAP v2.0	Wireless Application Protocol version 2.0; https://www.openmobilealliance.org	Mandatory	
WML v2.0	Wireless Markup Language version 2.0;	Mandatory	

POP3	Post Office Protocol 3 http://www.ietf.org/rfc1939.txt,2449.txt	Mandatory	
UDDI	Universal Description, Discovery, and Integration http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm#uddiv3	Mandatory	OASIS
Web Access standard			
WCAG 2.1	Web Content Accessability Guideline; version 2.1 https://www.w3.org/TR/WCAG21/	Mandatory	**W3C**

Ethiopian National Enterprise Architecture Framework (ENEAF) and Ethiopian eGovernment Interoperability Framework (EeGIF)

IMPLEMENTATION ROADMAP

MINISTRY OF INNOVATIONS & TECHNOLOGY | ADDIS ABABA, ETHIOPIA

Document Description

Document Title	Ethiopian National Enterprise Architecture Framework – Extension Implementation Roadmap
Document version	0.1
Document Status	**Draft**
Author(s)	Ermias Abebe Workshet Lamenew (PhD) Mesfin Kifle (PhD) Tibebe Beshah (PhD) Wondwossen Mulugeta(PhD)
ENEAF Decision	Under Review

Version Control

Version	Date	Description of changes made
0.1	03/11/2019	Draft document

Document Validation

Version	Authors	Reviewed by	Date	Status
0.1	ERMIAS ABEBE WORKSHET LAMENEW (PHD)	-	03/11/2019	DRAFT

List of Acronyms

ADM	Architecture Development Method
ARM	Application Architecture Reference Model
BRM	Business Architecture Reference Model
CIO	Chief Information Officer
DRM	Data Architecture Reference Model
EA	Enterprise Architecture
ERP	Enterprise Resource Planning
ESA	Ethiopian Standards Authority
ENEAF	Ethiopian National Enterprise Architecture Framework
FDR	Federal Democratic Republic (of Ethiopia)
GRM	Governance Reference Model
ICT	Information and Communication Technology
IRM	Integration Architecture Reference Model
MDA	Ministry, Department, Agency and Authority
MinT	Ministry of Innovations and technology (of the FDR of Ethiopia)
PMO	Prime Minister's Office
PRM	Performance Architecture Reference Model
SRM	Security Architecture Reference Model
TRM	Technology Reference Model
TOGAF	The Open Group Architecture Framework

Contents

1 Purpose of this Document

The ENEAF version 5.0 has been assessed to be a generic framework which should be translated into workable structures, processes, and tools. As part of the current update (2019), major changes were introduced to the framework so as to bring it one step nearer to implementation. Particularly, the

- Principles of the ENEAF were rationalized, streamlined and elaborated;
- A governing framework was proposed; and
- A compendium of standards to be adhered to developed.

The current update particularly focused on creating the basic infrastructure for realizing the national architecture. As such it focused on addressing the most relevant aspects of the "preliminary phase" of the ADM adopted as part of the ENEAF.

This roadmap document is developed to assist the planned and expedited realization of the national enterprise architecture. Its purpose is to indicate the major outstanding activities to be undertaken in the coming months and years. MinT, the MDAs, and the other organizations recommended in the governance structure could use this document as an input in their planning for a complete NEAF.

2 Audience of the Document

The main audience of this document are: MinT, MDAs, Governing Council, and Technical groups engaged in materializing the NEAF.

3 Project List

3.1 Establish Architecture Repository

Operating a mature Architecture Capability at a national level creates a huge volume of architectural output. Effective management and leverage of these architectural work products require a formal taxonomy for different types of architectural asset alongside dedicated processes and tools for architectural content storage. Therefore, MinT needs to establish a repository containing:

- All documents produced as part of the ENEAF development process
- Re-usable building blocks
- Publicly available reference models
- Organization-specific reference models
- Organization standards

3.2 Endorsement of Standards

As part of the current update, various standards are proposed to regulate the acquisition and/or development of data, applications, and infrastructures. These standards need to be endorsed by the Ethiopian Standards Authority (ESA).

3.3 Endorsement of the ENEAF

The ENEAF is developed in the interest of the nation. It is a mechanism and a tool for achieving efficiency and effectiveness in government. Therefore, the ENEAF (as updated) should be endorsed by the Council of Ministers for to gain formal acceptance by all stakeholders.

3.4 Establishment of organs defined in the governance structure

The governance structure developed as part of the current iteration of development of the ENEAF proposes several organs that could support its realization. Accordingly, the following organs need to be established at various levels of government.

- Governance Council under the PMO
- EA unit at MinT
- EA working groups at MDAs

To functionalize the governing organs, the processes and supporting documents need to be developed. Further,

- budget requirements and sources, and
- compliance guidelines and forms need to be worked out.

3.5 Elaborate the EA vision for the Federal Government (As-is)

The Governing Council and the technical working groups needs to set in motion a consultative process to frame the vision of the EA at the national level. Particularly,

- the visions, concerns and business requirements of the MDAs needs to be established;
- capabilities and readiness of the MDAs should be assessed;
- architectural principles for the MDAs need to be developed; and
- the top services that need to be delivered should be identified.

Based on the responses to the above questions, the governing council and the technical working groups could decide upon the scope, scale, timeframe and resource requirements of the overall effort. The exercise will create clarity on:

- the EA initiative that need to be prioritized;
- major components of the Core Platform;
- categorization of major applications as Common, Group and Domain-specific applications;
- number, nature and depth of performance parameters;
- sub-set of ENEAF principles and standards to be observed and enforced mandatorily;
- list of artefacts to be generated in the design and development of the Architecture;
- granularity of the design & documentation of the architectural artefacts;
- list of legacy applications to be leveraged;
- areas requiring BPR on top priority;
- integration goal and model;
- list of quick wins and game-changers to be targeted;
- high-level roadmap for implementation considering the above factors.

3.6 Elaborate the Reference Models of the ENEAF for the Federal Government (To-be)

Governance Architecture Reference Model (GRM): The objective of GRM is to manage and maintain architecture requirements and artefacts. It comprises of enterprise structure, processes and standards to ensure that the architecture is consistent with the business vision and objectives of the enterprise. Effective and efficient EA Governance ensures that priorities are based on broad consensus across the enterprise. EA is a continuous activity and governance is an integral part for its successful implementation and maintenance. As part of the current update, the ENEAF governance structure is drafted. However, the document needs to be iteratively completed through a continuous review process. In the next iteration, the governance architecture should address the following points.

- Integration of the EA governance process in the national procurement policy
- Funding model for future EA works. Particularly, emphasis should be given to the mechanisms by which regional states could be brought to the national EA fold.
- Stakeholder Consultation Strategy should be worked out to ensure the participatory nature of the EA development and governance process.
- The capacity building strategy should also be worked out. In this regard,
    - The Open Group could be engaged to certify Ethiopian Universities as local training centres. The Schools of Information Science of Addis Ababa University – as a unit of the AAU which helped enrich the ENEAF document – is well suited to serve as national training centre with other federal universities serving as regional cells.
    - Mechanisms for certifying MDAs, vendors, individuals should be worked out in collaboration with the aforementioned stakeholders.

Performance Architecture Reference Model (PRM): is designed to provide linkage between investments or activities and the strategic vision established by the Federal government and MDAs.

- Setup a mechanism by which MDAs publish their performance goals and measurement in machine readable format
- Establish a common repository to maintain performance data
- Establish process (and support documents) to allow for evaluation of investments based on alignment of IT investment to performance goals within an MDA and across MDAs
- Develop integration plan with BRM, ARM and DRM

Business Architecture Reference Model (BRM): it defines a functional view of Government's business processes, including the internal operations and services for citizens, the modes of delivering the services and enterprise back office processes. The BARM defines horizontal common business processes rather than MDA level stove piped view of processes.

- Government frontline and support services (portfolio)
- Service delivery modes and infrastructure plan
- Re-engineered processes

Application Architecture Reference Model (ARM): is a service driven view of the applications architecture defined to automate the business processes. The aim of the model is to recommend application services capabilities to support the reuse of business components and services across Government.

- Application portfolio
- Logical application architecture
- Service delivery channels with features
- Identity management and authentication management
- Develop portfolio of applications across MDAs to reduce cost of redundancy
- Integration plan for legacy applications
- Develop design artefacts for major processes

Data Architecture Reference Model (DRM): intended to promote the common identification, use, and appropriate sharing of data/information across the Government of Ethiopia through the standardisation of data. It defines the broad data entities across Government and their properties.

- Define government entities and their relationships
- Identify data sources across MDAs
- Define core data and meta-data
- Define data governance processes

Technology Architecture Reference Model (TRM): is technology driven model that categorises the standards and technologies to support and enable the delivery of service components and capabilities. The standards specifications and their policies have been defined in the e-GIF document.

- Network architecture topology for the government network infrastructure
- Create IT asset management strategy
- Identify opportunities for shared services

Security Architecture Reference Model (SRM): this defines the security framework that supports the applications and technical infrastructure to support the MDAs. Accordingly, the following activities should be undertaken as part of the SRM.

- Develop/update security policy
- Enforce application and infrastructure/technology with controls via standards
- Ensure Procurement guidelines and TOR/RFP documents include adopted security standards

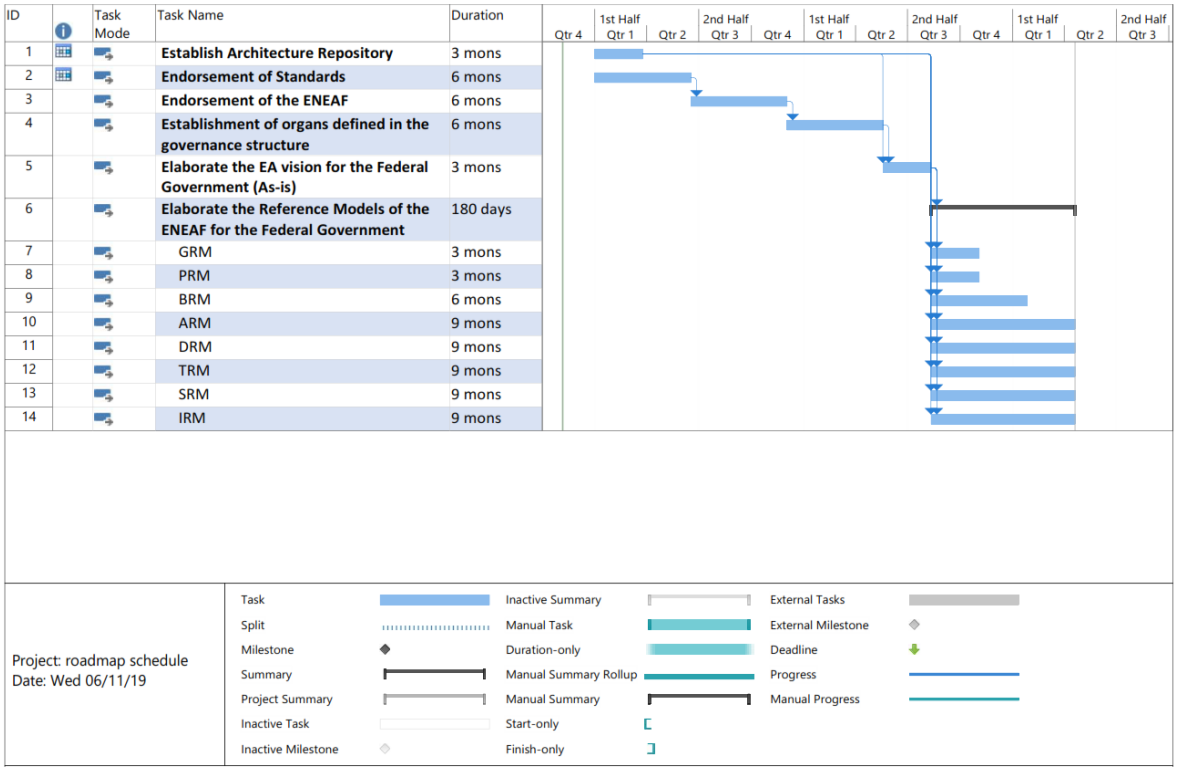
Integration Architecture Reference Model (IRM): A critical aspect of Enterprise Architecture in Governments is their ability to make government administrations at different layers to collaborate and work together in order to provide public services in an integrated seamless manner. When multiple government entities are involved there is a need for coordination and governance by the

relevant authorities with a mandate for planning, designing, provisioning, and operating public services. This makes integration architecture covering all the viewpoints (performance, business, data, application, technology, security) an absolute imperative to realize the vision of ONE Government. As part of the IRM, the following tasks should get attention by MinT and the governing council.

- Preparation and/or update of the E-government service bus document
- Launch of enterprise information integration project(s)
- Identification of shared ERP services and preparation of a plan for the acquisition of the same.

4 Time-Oriented Migration Plan

Project (major categories)	Estimated Duration for implementation
3.1 Establish Architecture Repository	3 months
3.2 Endorsement of Standards	6 months
3.3 Endorsement of the ENEAF	6 months
3.4 Establishment of organs defined in the governance structure	6 months
3.5 Elaborate the EA vision for the Federal Government (As-is)	3 months
3.6 Elaborate the Reference Models of the ENEAF for the Federal Government (To-be)[1]	
• **GRM**	3 months
• **PRM**	3 months
• **BRM**	6 months
• **ARM**	9 months
• **DRM**	9 months
• **TRM**	9 months
• **SRM**	9 months
• **IRM**	9 months



[1] It should be understood that EA at a national level is a long-term engagement. The duration estimate provided here is only for work at the level of the federal Ministries.

5 Risks and Issues

Management Buy-in: Buy-in at the top level of the government is the most critical prerequisite (and risk) for the successful materialization of the ENEAF. The ENEAF needs a champion promoter and that champion should preferably be from the top brass at the various levels of government. At the Federal level the support of the PMO should be assured. At the Ministry level, the endorsement of the Ministers or Vice Ministers is required.

Stakeholder Engagement: The extent to which all the stakeholders of ENEAF engage with the process will significantly affect the outcome. If there is a positive stakeholder attitude towards the whole endeavour, the process could be expedited, and the required change will materialize. Lack of acceptance or indifference to the project will ultimately make the ENEAF a white elephant – a project with big investment but no significant impact. Therefore, from the get-go MinT and other trend setters should set a strategy to engage all the stakeholders in the process.

Budget: The work spans over at least two fiscal periods and demands a significant amount resource. The Ministry should workout the detailed budget required for the work and look for funding sources.

Internal Capacity: Enterprise Architecting is new for many of our MDAs. The human and non-human capacity to support such change may not be available in many of the MDAs. The institutional capacity at all levels of government needs to be continuously assessed and wherever gaps are found, fast actions should be taken to remedy the deficiencies.

Approval/Endorsement Process: Several projects are suggested in this roadmap. However, implementing these projects in an agile manner instead of in a sequential waterfall is recommended. Quick wins always help to capture the trust of stakeholders. Therefore, the governing council should move to establish the essential building blocks of the architecture before the detailed elaborations are launched.

Technological changes: Technological changes are always a threat to any planned change. Constant monitoring of the environment is required to keep abreast with the changes. The standards, structures, tools, techniques, and infrastructures need to be updated. The ENEAF should remain a work in progress to stay fresh.

Political Changes: As indicated in the first bullet, top management commitment is the top most criteria for the success of ENEAF. However, the government may change its focus from time to time which means the ENEAF may lose its credibility and potency. The best strategy to mitigate this risk is to continuously align the ENEAF with the policies and strategies of the sitting government. Promotion and popularization could also make the ENEAF current in the minds of all the stakeholders.

Governance process: The speed with which the governance structure processes requests and develop & implement architectural changes could make or break the ENEAF. The governance council, the technical working groups and the coordinating unit within MinT should serve as change agents instead of bureaucratic hurdles. A continuous participatory process with all stakeholders could help clear misunderstandings and positively frame the working modalities of the governing organs.