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.

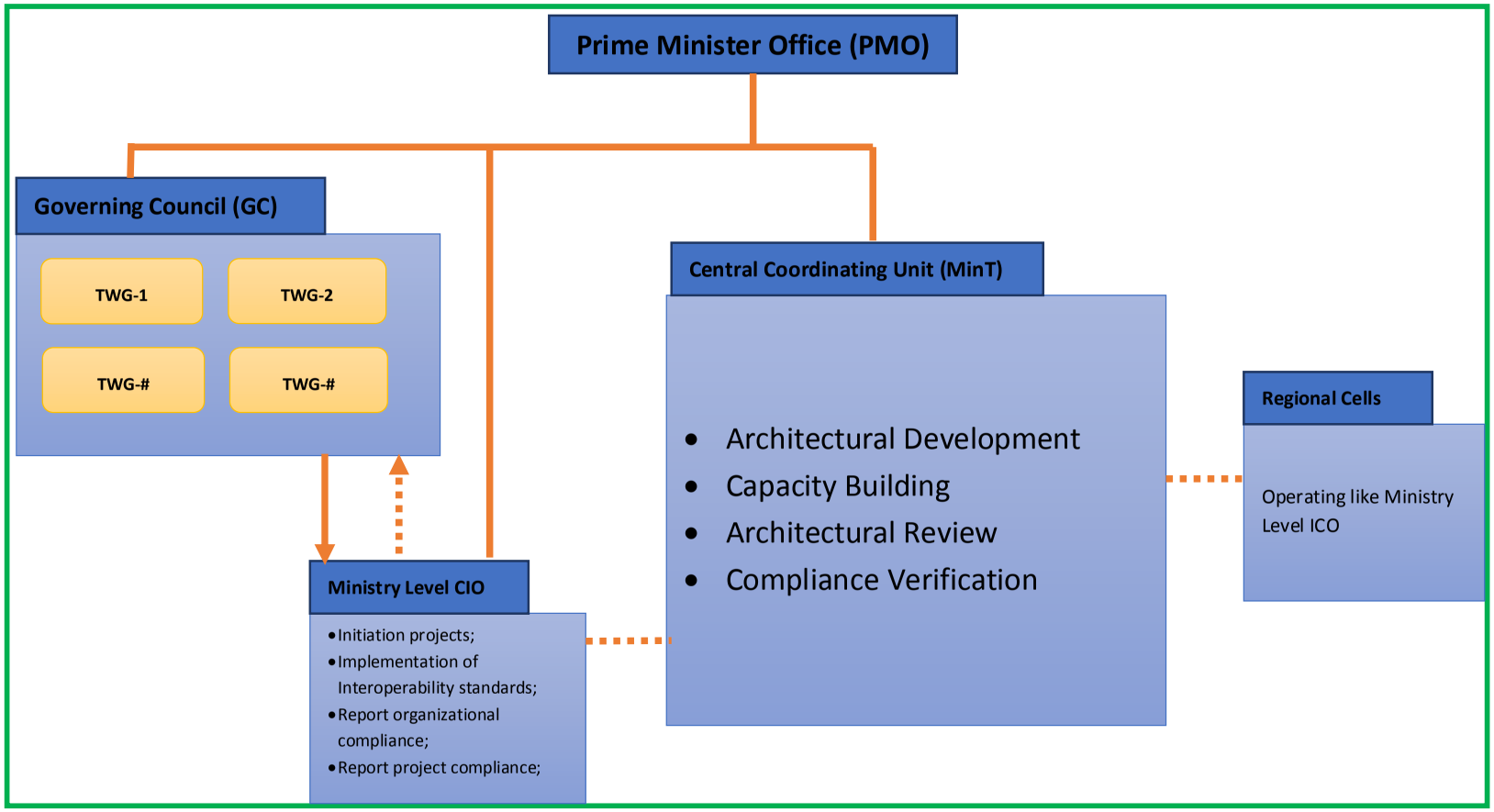

Figure 1: Proposed ENEAF and EeGIF Governance Structure

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.

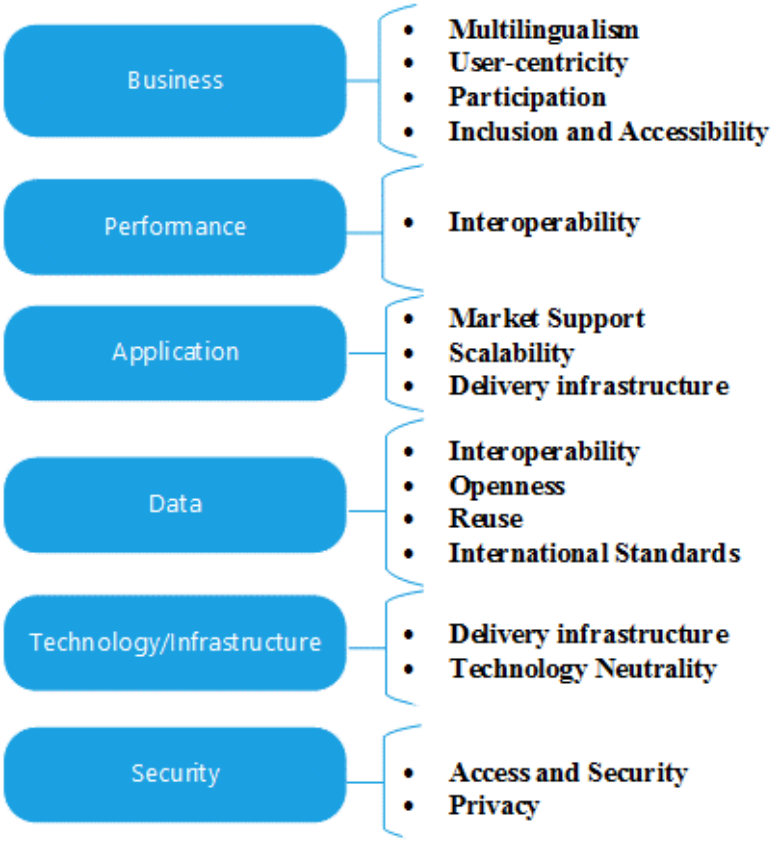

Figure 3: EeGIF Guiding Principles

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.

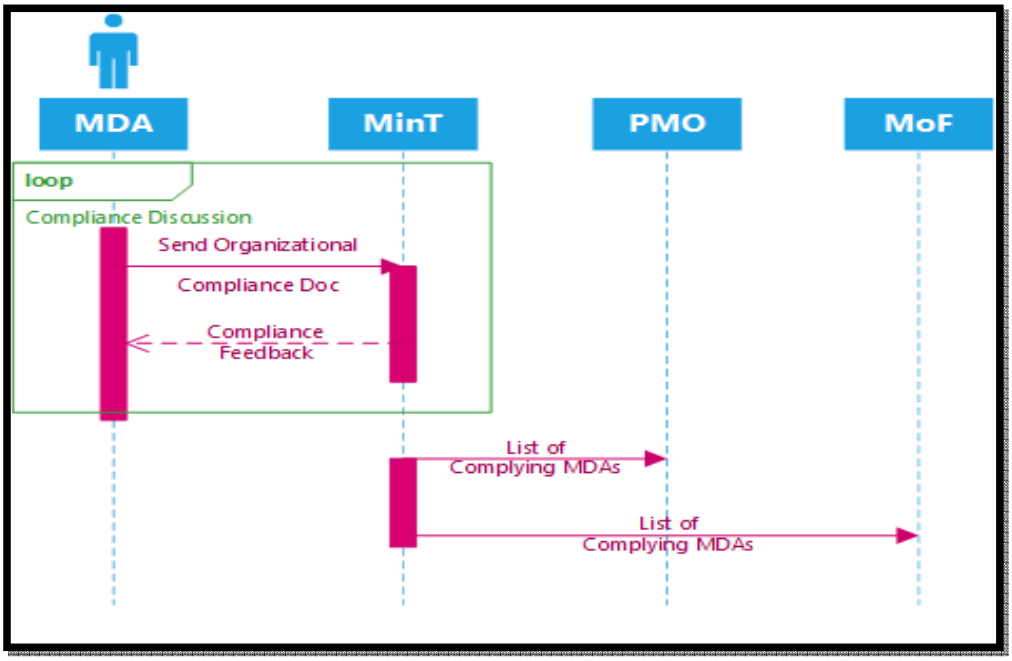

Figure 4: Organizational Compliance Activity Diagram

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.

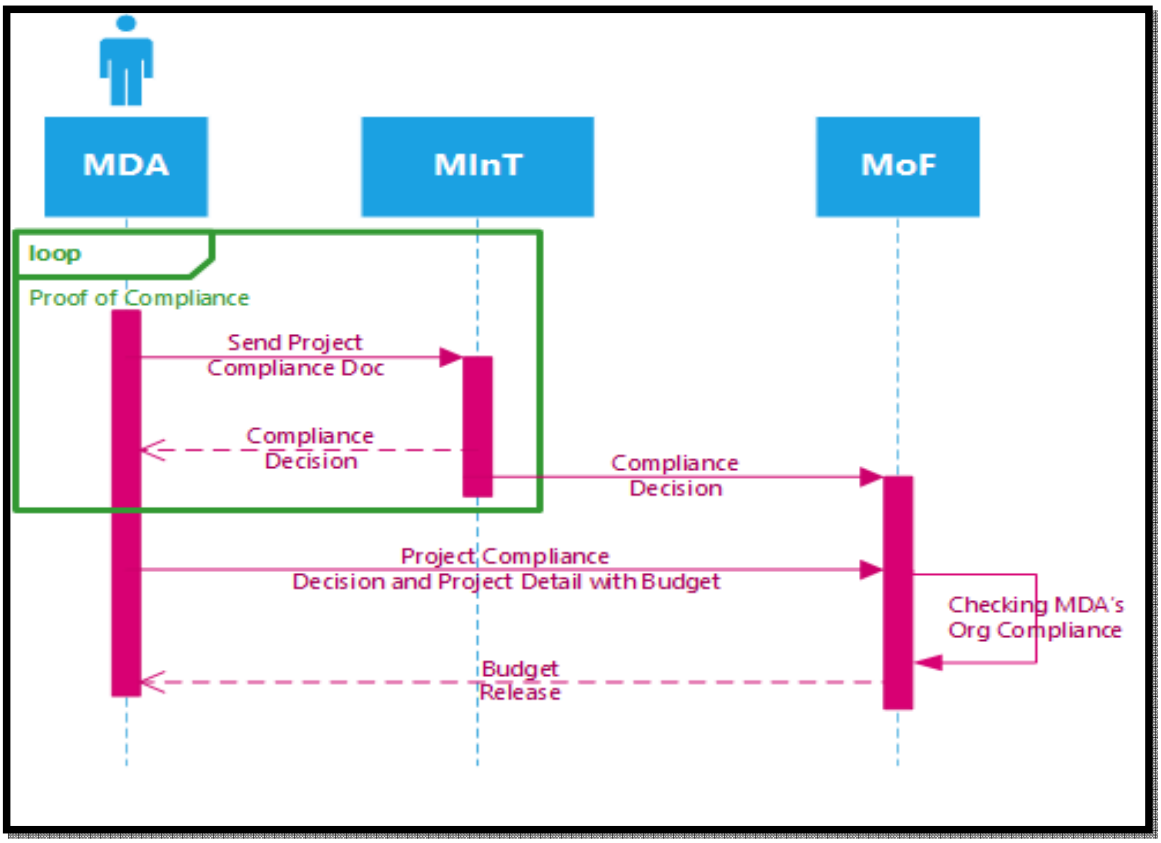

Figure 5: Project Level Compliance Activity Diagram

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.