



Ghana Government eGovernment Interoperability Framework (eGIF) Assessment Methodology Report

Table of Contents

1.	Introduction.....	5
2.	eGIF Stakeholders.....	5
2.1	eGIF Advisory Board.....	5
2.2	Working Groups.....	6
2.3	Change Requestor	6
3.	The eGIF Change Management	8
3.1	eGIF Change Management	8
3.2	Classification of Changes	8
3.3	Types of Changes.....	8
3.3.1	eGIF Technical Standards and Policies Change Process	9
3.3.2	Change Process for eGIF XML and Metadata.....	9
3.4	Configuration Management	13
4.	The Assessment for Compliance	14
4.1	Types of Assessments	14
4.1.1	Annual Assessment Process.....	14
4.1.2	Project/ Ad-hoc Assessment Process	15
4.2	Scope of Assessment.....	16
4.2.1	Channels Interoperability Assessments	16
4.2.2	Business Process Interoperability (BPI) Assessments	17
4.2.3	Network Interoperability Assessments	18
4.2.4	Service Oriented Architecture (SOA) Assessments	19
4.2.5	Data Interoperability Assessments.....	20
4.2.6	Security Interoperability Assessment	21
5.	Enforcement.....	22
5.1	e-GIF Maturity Management.....	22



1. Introduction

The e-Government Interoperability Framework (eGIF) is at the heart of Ghana Government's drive to modernise government through the introduction of appropriate technologies. The role of the eGIF is to establish government wide framework for the management of technical standards, policies, XML Schemas and the metadata model to ensure consistent exchange of information across government.

eGIF assessment methodology is a process of measuring how government Ministries Departments and Agencies (MDAs) information systems conform to the policies and standards outlined in the eGIF policy and standards catalogues. In order to achieve interoperability, there must be a coherent alignment between the eGIF policies and standards and the systems implemented by the MDAs.

This report describes the methodology to be used by GICTeD and other stakeholders for the assessing eGIF standards and policies, the management of changes to the eGIF and ensuring compliance by the MDAs. The main purpose of the report is to provide a methodology that defines the roles, decision points and the steps for keeping the eGIF up to date and ensure that all technology deployments across government meet the approved standards. The report identifies an assessment model, which defines the different Working Groups for the different eGIF domains (Technical Standards, Policies, XML Schemas, and Metadata Model), their roles and responsibilities and the change control processes. It discusses the compliance and enforcement processes and the key stakeholders involved.

The report also provides the framework that will help to carry out both routine and adhoc (or project based) assessment of eGIF standards and policies for compliance. The document outlines the various bodies (Working Groups) that need to be set up to oversee the assessment of the standards and policies for the various interoperability areas.

2. eGIF Stakeholders

Industry best practice indicates that eGIF assessment should be carried out according to a governance model, which will provide the key ingredients for managing interoperability across government in an effective manner. The eGIF will be generally owned by GICTeD but a number of Working Groups and an Advisory Board will be set to oversee the development, maintenance, monitoring and promotion of the standards policies and other key components. The roles of the stakeholders are:

2.1 eGIF Advisory Board

The eGIF Advisory Board will be set up under GICTeD to oversee eGIF as an independent body, separate from the domain Working Groups. The board must be seen as experts in the field of interoperability to ensure trust and will work collaboratively with MDAs to ensure eGIF is maintained and used effectively across government. Other roles and responsibilities of the board include:

- Proactively promoting eGIF use across government;



- Monitoring eGIF usage and policing adherence to standards and policies;
- Advisory body for the MDAs implementing their Enterprise Architecture to provide advice on how to ensure eGIF standards are incorporated into their technology blueprint;
- Ensuring cross MDA interoperability and resolving issues associated with interoperability;
- This consultative body meets regularly to access, prioritise and plan changes. Board membership includes representatives appointed by GICTeD from the public and private sectors;
- Defining intellectual property rights constraints to prevent manipulation of standards by vendors for market dominance.

2.2 Working Groups

To maintain the eGIF the following Working Groups must be established to be responsible for all changes and updates to the various domains of the eGIF. This includes the management of standards, policies, specifications etc. The Working Group membership will comprise of selected individuals from the public sector, private organisations and industry subject matter experts all appointed by GICTeD.

Capacity building is an important objective of the eGhana project and as such it is critical that the Working Groups undertake efforts to disseminate information as well as to educate and train MDA staff on eGIF and its standards.

The following Working Groups must be formed;

- **Technical Standards & Policies** - this group will be responsible for the coordination of all changes pertaining to the technical standards, specifications and policies defined in the eGIF. The primary role of this group is to assess and enforce technical interoperability. This group will also be responsible for studying industry standards as they are used and make the necessary recommendations for their use in Ghana.
- **XML Schemas** - this group is responsible for setting of specifications, and the coordination of maintenance of the government XML Schemas. The group will develop and approve all schemas to be used across the public sector. They will advice and facilitate the development of common schemas across government. The group will be made up of experienced representatives across MDAs and the private sector with data management experience. All requests for changes and assessments to be carried out in relation to the schemas will be handled by this group. All schemas reviewed and approved will be published on the eGIF website and made available for use.
- **Metadata Model** - this group will provide advice on all aspects of the metadata model and will develop and maintain the metadata model across government.
- **Other Special Interest Groups** - wherever necessary GICTeD will set up Working Groups on adhoc basis to formulate policies and standards for specific technical areas, including emerging technologies.



2.3 eGIF Change Requestor

A Change Requestor is any individual or organization that initiates changes to the different components of the eGIF. The Request for Change could be initiated by:

- ☐ MDAs
 - Enterprise Architect;
 - Chief Information Officer/ICT Director;
 - Other technical staff.
- ☐ Citizens
- ☐ Industry Experts
 - Vendors
 - Analysts/consultants
- ☐ GICTeD
- ☐ Working Groups



3. eGIF Change Management

The Assessment should cover all the life cycle stages of the eGIF implementation:

- Initiation stage: the current stage in which the eGIF is in its early stage. In this case there is a need for a check list of eGIF implementation: establishment of the various committees, collection of requirements etc
- Design and implementation: what are the foundations which need to be in place to build the eGIF implementation: Assessment of BRM, DRM, Security foundation, Networking foundation assessment, basic standards which need to be developed / adopted by the various committees, policies and regulation assessment.
- Mature stage / Maintenance stage: at this stage the foundation of an interoperable e-Government solution is in place and the government of Ghana is ready to deploy application. Assessment of new application change of applications.

3.1 The Change Management Process

Change is a fact of life and eGIF specifications and policies will change overtime. GICTeD must ensure changes can be applied effectively and rapidly. It is GICTeD's responsibility to ensure that eGIF is up to date and consistent with industry trends and stakeholder needs. The GGEA and eGIF Portal will provide the workflow for and content repository for the eGIF artefacts.

The Change Management process is designed to encourage widespread participation and the need to be able to apply changes rapidly. It also describes how changes to the various eGIF components will be managed. Changes to the XML Schemas and the Metadata model will be treated as special cases due to the potential impact the changes can have on MDAs. As a result changes to the agreed XML Schemas and the Metadata model need to be managed carefully, with proper procedures in place to ensure that all involved parties to the change are properly consulted and agree to the change. The idea is to reduce the impact of change on existing applications that use the XML Schemas.

3.2 Classification of Changes

The two main eGIF change types are:

- ☐ Planned changes that are applied annually after a review. The eGIF Advisory Board will ask the Working Groups to review their domains and submit their Request for Changes. The technical standards and policies will be revised annually, subject to the government's future ICT direction.
- ☐ Ad-hoc changes are made due to errors, or changes to industry specifications that need to be applied as soon as possible.

3.3 Types of Changes

There are two kinds of change processes that can be initiated and they are:

- ☐ eGIF Technical Standards and Policies Change Process;
- ☐ eGIF XML and Metadata Model Change Process;



The distinction is due to the more rigorous nature of the change process pertaining to the XML Schema and the Metadata Model.

3.3.1 E-GIF TECHNICAL STANDARDS AND POLICIES CHANGE PROCESS

The change process for the eGIF Technical Standards and Policies is initiated when a Requestor, requests for a change. Upon the request a decision as to the type of change is determined.

If the change is a Technical Standards and Policies change, it's forwarded to the Technical Standards and Policies Working Group for assessment, and then a check is made in the eGIF Configuration Management Database in the Portal to ascertain the existence of the said standard or policy. The eGIF version is also established to ensure version control of the artefacts is maintained.

If a policy or standard already exist, it is checked against industry standards and then published on the eGIF Portal for comments.

Based on the comments, a recommendation is made to the eGIF Advisory Board for validation and approval. On approval, the change is adopted and, the Configuration Management Database is updated and forwarded to the appropriate technical teams for implementation. The changes are then published on the GICTeD eGIF website and the process ends. Else an outline of the reasons why a request for change was not approved is sent to the Requestor. Figure 1 below illustrates the Technical Standards and Policies change process.

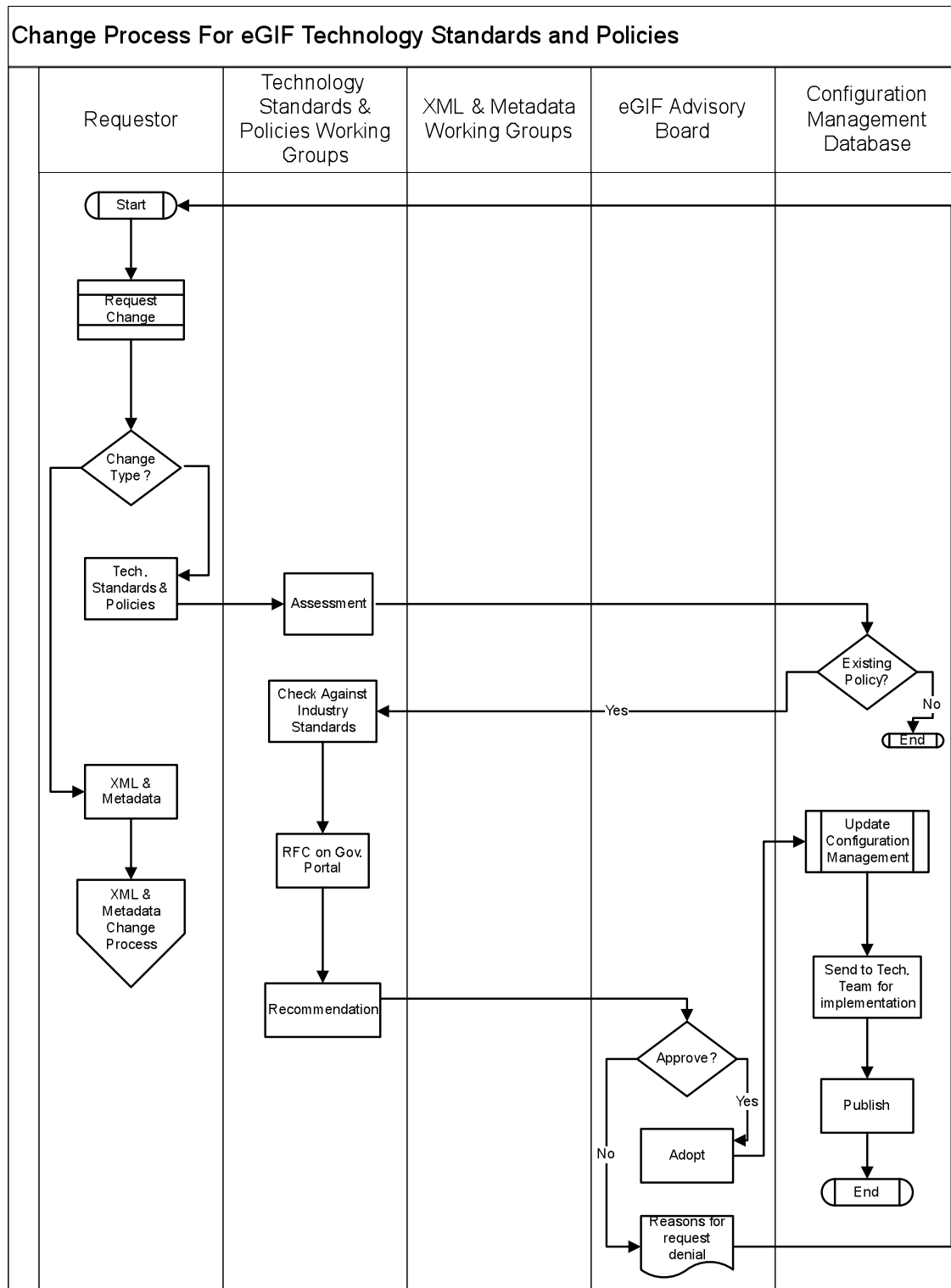


Figure 1: eGIF Technical Standards & Policies Change Process



3.3.2 CHANGE PROCESS FOR eGIF XML AND METADATA

The change process for the eGIF XML Schema and Metadata Model is initiated when a Requestor, requests for a change. Upon the request a decision as to the type of change is determined.

If the change relates to the XML Schema or the Metadata Model the change is passed to the appropriate Working Group for assessment who will check that eGIF XML Schema stored in the XML Configuration Management to establish details of the XML involved and ascertain the extent of impact.

If the schema or metadata model already exists, it is checked against the various data models to establish the required changes and agencies could be affected as well as applications services involved. The analysis conducted by the Working Group will then be published on the GGEA and eGIF portal for comments.

Based on the comments a recommendation is made to the eGIF Change Advisory Board for approval. On approval, the change is adopted and the XML or Metadata Configuration Management Database is updated and forwarded to the appropriate technical team for implementation. The changes are then published on the GICTed eGIF website and the process ends.

Else an outline of the reasons why a request for change was not approved is sent to the Requestor. Details of the XML and Metadata model change control process is illustrated in figure 2 below.

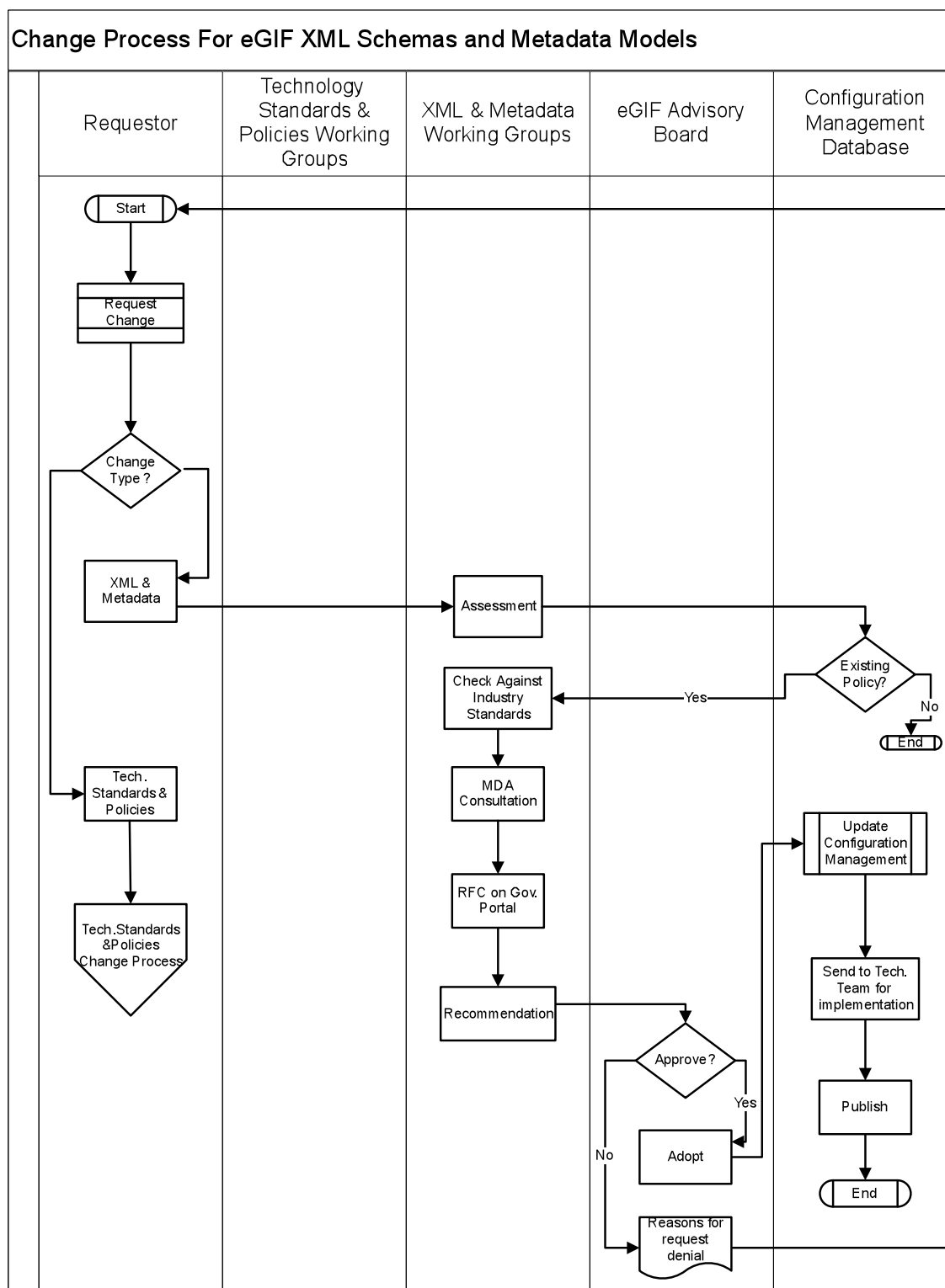


Figure 2: eGIF XML Schema & Metadata Model Change Process



3.4 eGIF Configuration Management

This process is concerned with the version control management of the eGIF artefacts. Configuration Management in this case is similar to the traditional software configuration management, which is used to handle changes in software projects. The eGIF Configuration Management identifies the different versions of the eGIF artefacts stored at various points in time, and provides the mechanisms for controlling changes for the purpose of maintaining the integrity and traceability throughout the eGIF management life cycle.

The eGIF Configuration Management database is basically a data store on the eGIF Portal for the various artefacts with an effective version control and numbering process, which will make it easier to trace changes, and provide the ability to verify that the right versions of the artefacts are stored. The version numbering standard for the eGIF components will be V.01, which will be changed when a new release of the eGIF component is approved and implemented.



4. The Assessment for Compliance

This assessment methodology is to help determine whether or not an MDA's IT infrastructure is eGIF compliant. E-GIF compliance by MDAs will not be easy to achieve if assessment for compliance is complicated and not linked to an investment appraisal process. eGIF compliance must be mandated and linked with the allocation of ICT budgets across government and this will ensure that the necessary standards and policies are adopted before the ICT team can get approval to spend on e-government projects. For this to be effective government must have full visibility of planned projects and effective control over the use and disbursement of ICT funds.

MDAs must receive annual awards or recognition for eGIF compliance and the promotion of re-use. This is also an effective way of encouraging or promoting eGIF compliance. The eGIF Working Groups will have a major role to play in promoting eGIF compliance by supporting MDAs to go through the process of adoption and use of the eGIF standards. The groups will also advise MDAs of emerging standards and publish reference manuals that describe how to build eGIF-compliant systems. MDAs will be taken through the entire process of ensuring eGIF standards and specifications are incorporated into the design and implementation of systems. This section describes the different types of assessment methods and the scope of assessing the different interoperability areas with examples of assessment reports, which will be published on the eGIF portal.

4.1 Types of Assessments

There shall be two types of assessments for compliance to be conducted by GICTeD (assessment team). This will comprise of a comprehensive annual assessment of MDA IT infrastructure's compliance to eGIF. The second type of assessment is where MDAs are expected to submit a comprehensive report on any major ICT project they want to undertake. The report should spell out the technologies to be deployed, versions and XML schemas and meta-data standards to be used. This will enable GICTeD to carry out a thorough project assessment to confirm that the technology to be deployed meet the agreed standards and policies outlined in the eGIF working document. The two assessment types are described below.

4.1.1 ANNUAL ASSESSMENT PROCESS

It is recommended that an annual assessment of MDA ICT infrastructure is carried at a specified time. Each MDA will be required to submit an annual inventory of their ICT portfolio clearly outlining all deployed systems, the supporting technologies and their versions. In addition any planned projects to be deployed in the future are to be included for eGIF compliance assessment. The GICTeD Assessment team will also conduct policy reviews annually whereby they will discuss architectural requirements and the eGIF policies to support them. The team will assess that MDAs have adopted the eGIF policies and have incorporated them into systems design.

There should also be an agreed time between GICTeD (Assessment Team) and the MDAs for assessment team to assess their ICT infrastructure. This will enable GICTeD as a governing body to follow up after the assessment to ensure specifications are being used as defined in the ICT inventory.

The assessment process will be conducted through the eGIF & GGEA Portal, whereby GICTeD will send a formal request for eGIF compliance review. On submission of the request the MDA



will send the inventory list through the Portal providing GICTeD an audit trail of compliance reviews. The Portal's internal workflow will allow the various Working Groups to be included in the review process.

We recommend all MDAs to have an annual internal ICT audit, which will conduct audits for compliance. This will help the MDAs build the necessary internal systems for eGIF compliance prior to the GICTeD review.

4.1.2 PROJECT/ AD-HOC ASSESSMENT PROCESS

Ad-hoc assessments will be performed when major systems are to be deployed by MDAs. This assessment will be carried out when the MDAs initiate ICT projects. A 'gating' process (as illustrated in figure 3) must be implemented to review and approve projects for eGIF compliance. Compliance 'gates' are review points in the systems development life cycle (SDLC) when Project Managers will be required to submit eGIF compliance reports for review.

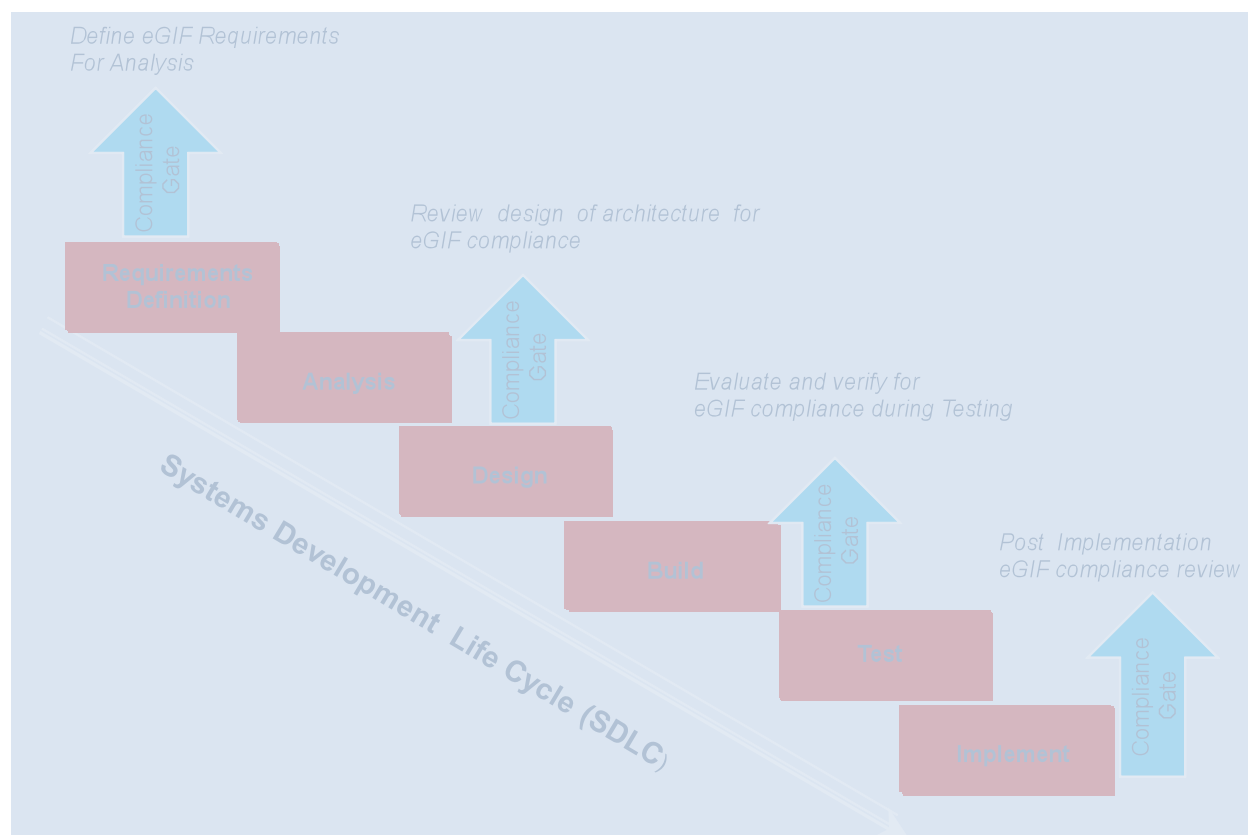


Figure 3: Project eGIF Compliance Gates

The eGIF compliance 'gating' reviews will be conducted as following:

- **Define eGIF Requirements for Analysis** – this compliance 'gate' review occurs during the Requirements Definition phase to ensure that eGIF requirements are captured for analysis. This will ensure that standards, specifications and policies are adopted right at the beginning of the project.



- **Review Architecture Design for Compliance** – during systems design a review of the architecture will be conducted to ensure that system components meet eGIF standards and policies are also incorporated into the design of the system prior to the Build stage.
- **Evaluate and Verify for eGIF Compliance** – during the testing phase the project team will be required to verify that all components meet eGIF standards. This is required before system is allowed to be implemented.
- **Post Implementation Review for Compliance** – this could be a randomly performed review by GICTeD to verify that components and specifications are what were tested for implementation from a compliance standpoint.

MDAs implementing major computer systems will be required to submit eGIF review reports and projects could be stopped if they have not followed the original technical specifications. Random inspection of major ICT projects is also an effective way of enforcing eGIF standards.

4.2 Scope of Assessment

Although there are many attributes that describe the requirements of an information system, the eGIF assessments will be centered on interoperability. The attributes of interoperability to be considered under eGIF assessment need to be relevant and well defined. The assessment will be carried out by identifying the relevant policies and standards from the eGIF policy and technical standards catalogue (at least those which have the status of Adopted or Recommended) in the areas of:

- Channels Interoperability;
- Business Process Interoperability;
- Network Interoperability;
- Service Oriented Architecture (SOA);
- Data Interoperability;
- Security Interoperability.

4.2.1 CHANNELS INTEROPERABILITY ASSESSMENTS

MDAs will be required design system interfaces and channels for citizens to access their services. The Enterprise Architecture defines a wide range of channels through which the government can disseminate information and the systems to be developed by the MDAs need to be assessed to ensure they are capable of supporting secure, safe and efficient delivery channels, either directly or via third-party services.

The delivery channels of the MDAs must be accessed based on the policies outlined in the Ghana Government e-GIF Policy document. The table below provides an example of the assessment reports that could be generated for channels interoperability assessments. .



Table 1: Channels Interoperability Assessment Example report

Channels	Specifications	Remarks (Official)
This column outlines the various channels present at the MDAs and the technology standards they support. E.g. Internet ☐ Hypertext interchange formats ☐ Document file types	This column outlines the specifications of the various channels standards. These include the versions and unique capabilities. HTML v3.0 File extensions (.rtf, .txt, .htm/.html, .pdf, .doc, .nsf, .mht)	This column is reserved for auditor's use. This may be 'Approved' or 'Not Approved' Not Approved (HTML v4.01) Approved

4.2.2 BUSINESS PROCESS INTEROPERABILITY (BPI) ASSESSMENTS

The delivery of services across MDAs and citizens requires business process standardisation, which will provide the framework for an efficient and effective connection between MDAs to be able to interoperate. Making sure business processes are streamlined to conform to lay down standards and processes is crucial in achieving this aim.

Business process assessment criteria should be dynamic due to changing needs of customers. The policies and standards must be changed and fine tuned from time to time.

The table below shows an example of BPI assessment for eGIF compliance report.



Table 2: BPI Assessment Example

BPI	Specifications	Remarks(Official)
This column outlines the various business processes present at the MDA and the technology standards they support. E.g. Human Resource Management ☐ HRM ☐ Business Object Documents	This column outlines the specifications of the various BPI standards. These include the versions and unique capabilities. HR-XML ebXML	This column is reserved for auditor's use. This may be 'Approved' or 'Not Approved' Approved Approved

4.2.3 NETWORK INTEROPERABILITY ASSESSMENTS

Network Interoperability is the continuous ability to send and receive data between interconnected MDA networks, providing the level of quality expected by citizens and employees who are the end users without any negative impact to the IT services. The criteria for assessment or the minimum requirements to pass the network assessment should be the requirements outlined in the Ghana Government e-GIF Technical Standards Catalogue. The criteria needed to assess the interoperability of MDA networks include the following:

- ☐ Internet Accessibility;
- ☐ Wireless Networks;
- ☐ Next Generation networks (NGN);
- ☐ Content Distribution Network (CDN).



The table below provides an example of the report that could be generated from Network Interoperability assessment.

Table 3: Network Interoperability Assessment Example

Networks	Specifications	Remarks(Official)
This column outlines the various networks present at the MDA and the technology standards they support. E.g. Wireless Network ☐ Wireless LAN ☐ Security ☐ WAN ☐ Hypertext transfer protocols	This column outlines the specifications of the various channels standards. These include the versions and unique capabilities. WEP IP v4.0 HTTPv1.1	This column is reserved for auditor's use. This may be 'Approved' or 'Not Approved' Approved Not Approved (IP v6.0) Approved

4.2.4 SERVICE ORIENTED ARCHITECTURE (SOA) ASSESSMENTS

This is a new concept in the world of interoperability and the underlying principle behind the concept is the idea that IT systems, software, devices and services should integrate and “talk” to each other even if they were never specifically designed for each other in the first place.

SOA is implemented using Web services. Thus, the criteria for SOA assessment is largely Web standards related. The key levels for assessing SOA are:

- ☐ Web services - which handles the application space, together with associated management and business processes;
- ☐ Applications and applications infrastructure;
- ☐ Foundation - handles messaging, security, reliability, transactions and metadata;
- ☐ Transport - based on transport protocols such as HTTP, UDP, TCP, SMTP and so on.

The detailed policies and standards for these levels can be referenced in the policy framework of the Ghana Government eGIF. The table below provides an example of SOA interoperability assessment.



Table 4: Service Oriented Architecture (SOA) Assessments Example

SOA	Specifications	Remarks(Official)
This column outlines the various SOAs present at the MDA and the technology standards they support. E.g. Web Services ☐ Web service request delivery ☐ Web service description language ☐ Web service request registry	This column outlines the specifications of the various channels standards. These include the versions and unique capabilities. SOAP v 1.0 WSDL 1.1 UDDI v 2.0	This column is reserved for auditor's use. This may be 'Approved' or 'Not Approved' Not Approved (SOAP v 1.2) Approved Not Approved (UDDI v 3.0)

4.2.5 DATA INTEROPERABILITY ASSESSMENTS

Data assessment measures how data is handled across government from input, processing, output and storage. The assessment ensures the processing of data is in compliance to the policy framework of the Ghana Government eGIF.

Table 5: Data Interoperability Assessment Example

Data	Specifications	Remarks(Official)
This column outlines the various Data Integrations present at the MDA and the technology standards they support. E.g. Data Integration ☐ Metadata/Meta Language ☐ Data transformation	This column outlines the specifications of the various channels standards. These include the versions and unique capabilities. XML XSL	This column is reserved for auditor's use. This may be 'Approved' or 'Not Approved' Approved Approved



4.2.6 SECURITY INTEROPERABILITY ASSESSMENT

The security of data across government is one of topmost priority. Thus, there is the need to critically assess and make sure systems deployed by MDAs are secure. Information security is the process of ensuring the confidentiality, integrity and availability of government information.

The security assessment criteria should be based on the following:

- ☐ Network infrastructure and services - Transport level security, e-mail security, network level security, wireless network security, network encryption;
- ☐ Data security - privacy policy and identity management.

Table 6: Security Interoperability Assessment Example

Securities	Specifications	Remarks(Official)
This column outlines the various Securities present at the MDA and the technology standards they support. E.g. Network Security ☐ Transport-level security ☐ IP network-level security	This column outlines the specifications of the various channels standards. These include the versions and unique capabilities. SSL v1.0 IPsec	This column is reserved for auditor's use. This may be 'Approved' or 'Not Approved' Not Approved (SSL v3.0) Approved



5. Enforcement

In Ghana a government legislation may be necessary for eGIF enforcement and the law should be broad enough to empower an agency to secure compliance, but not overly specific about standards. Specific standards should be defined in regulations, since it is very difficult to update and retire standards if they are legislated. The need for legislation to enforce eGIF in Ghana is based on the fact that there are challenges such as:

- ☐ The level of bureaucracy and the nature of bureaucracy;
- ☐ The autonomy enjoyed by MDAs;
- ☐ The lack of accountability of different MDAs;
- ☐ IT skills shortage in government.

Any MDA that fails to comply with the assessment process or do not meet the assessment criteria must attract some penalties. The penalties may include the following:

- ☐ eGIF assessment must be a key criterion used by government and other donor agencies in sponsoring ICT projects. Any form of sponsorship must be withheld if the project is considered not be aligned with the government's approach to interoperability.
- ☐ New systems that fail to comply must not get project approval from appropriate authorities. Example, the Public Procurement Authority (PPA) as part of its mandate must also ensure that all projects submitted for the procurement process are eGIF compliant before approving them for the tender process.
- ☐ Vendors who do not meet the specifications of eGIF must be blacklisted and supplies terminated.
- ☐ Systems that fail to meet specifications must not be allowed to be connected to any middleware technologies for data exchange or be part of shared services.

5.1 eGIF Maturity Measurement

The degree of success in terms of the level of interoperability achieved by the MDAs is very important for e-government implementation in Ghana. The measures required to address the level of interoperability are:

- ☐ Technical compliance measures;
- ☐ Systems interoperability measures;
- ☐ Operational interoperability measures;
- ☐ Organizational and cultural measures.

eGIF Interoperability Certification based on maturity levels is also another possible enforcement mechanism available to GICTeD. Certification based on the level of interoperability or its maturity in the organisation will be awarded to the MDAs. The annual eGIF compliance 'awards' or events is when certificates will be given to eGIF compliant MDAs. The certification



event also provides the opportunity for the government to know about the non-eGIF compliant MDAs.

The eGIF Interoperability Certification process will be based on an Interoperability Maturity Model, which consists of five levels and a number of eGIF characteristics. The general five levels are described below:

- **Level 1 (None)** - either an organisation does not have plans to develop and use eGIF, or it has plans that do not demonstrate an awareness of the value of having and using eGIF. While Level 1 MDAs may have initiated some eGIF activity, their efforts are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation necessary for successful eGIF development.
- **Level 2 (Beginning)** - An organisation at Level 2 recognises that the eGIF is linked with ICT funding process and the developing of its Enterprise Architecture (EA) to drive the technology deployment strategy. The EA definition process also includes the adoption of the eGIF standards and policies to ensure compliance.
- **Level 3 (Established)** – MDA at Level 3 focuses on developing architecture products according to the selected Enterprise Architecture framework, methodology, tool, and established management plans. The MDA has established the eGIF strategy and has at least established and adopted the Channel and Business Process Interoperability standards and policies. Although the products may not be complete, they are intended to describe some of the e-services to be implemented.
- **Level 4 (Improved)** – MDA at Level 4 has completed its full eGIF adoption as part of the EA definition process. The completed eGIF products collectively are based on the following interoperability areas:
 - (1) Channels Interoperability;
 - (2) Business Process Interoperability;
 - (3) Network Interoperability;
 - (4) Service Oriented Architecture (SOA)
 - (5) Data Interoperability;
 - (6) Security Interoperability.
- **Level 5 (Optimised)** – MDA at Level 5 has secured approval for all the interoperability areas, the MDA fully utilises the government XML Schema, the Metadata model and all technical standards and policies. The MDA is able to exchange data seamlessly with other MDAs and private sector organisation using the eGIF standards and specifications to achieve interoperability. All ICT investments comply with eGIF, unless granted an explicit compliance waiver. Also at Level 5, the organisation tracks and measures eGIF compliance internally as part of the ICT audit function and uses the GICTeD assessment methodology to ensure overall compliance.



We provide a summary of the eGIF assessment levels in the table below.

Table 7: Assessment levels summary

Level	Description	EA Characteristics
1	None - No eGIF process in place	1. No eGIF exist or yet to be defined 2. No structures in place to develop EA
2	Beginning – eGIF process is being developed	1. Recognises that eGIF is linked to ICT funding process. 2. Begin the process of defining EA to incorporate eGIF standards
3	Established – eGIF definition process has commenced	1. eGIF is being defined as part of the EA process 2. Some eGIF areas such as channel interoperability and Business Process Interoperability have been defined 3. ICT procurement is governed by eGIF standards
4	Improved – eGIF process is managed and measured	1. eGIF includes all the different Interoperability areas (Channel, Business Process Interoperability, Network Interoperability, Service Oriented Architecture (SOA), Data Interoperability, Security Interoperability
5	Optimised – Continuous improvement of the eGIF process	1. MDA achieves full interoperability with other MDAs and private sector organisations 2. Internally ICT audit function in place 3. Uses standard assessment methodology for eGIF compliance and optimisation