



the dpsa

Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

MINIMUM INTEROPERABILITY STANDARDS (MIOS) for Government Information Systems

Revision 5.0

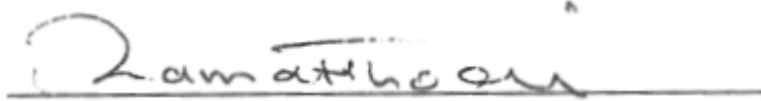
APPROVAL

I, the undersigned –

in terms of the Public Service Act (Act 38 of 1994 as amended by Act 30 of 2007) sections 3(1)(f) and 3(1)(g) regarding electronic government norms and standards and the Public Service Regulations 2001 (as amended 2001 to 2010) Chapter 5, Part I and Part III, and the State Information Technology Agency Act (Act 88 of 1998 as amended by Act 38 of 2002) sections 7(6)(a)(i) and 7(6)(b) regarding interoperability standards and certification; and

after consultation with the Government Information Technology Officer's Council (GITOC), hereby approves and issues the Minimum Interoperability Standard (MIOS) for Government Information Systems version 5.0; and

that the MIOS v5.0 supersedes and replaces all previous versions thereof, and be effective and must be complied with in terms of Public Service Regulations Chapter 5, Part III as from the date of signature.



MINISTER: PUBLIC SERVICE AND ADMINISTRATION

Adv. Ngoako A. Ramatlhodi *(02), MF*



Date

PUBLICATION ENQUIRIES

The Minimum Interoperability Standards (MIOS) for Government Information Systems is developed by the State Information Technology Agency (SITA): Standards and Certification Unit in consultation with the Government Information Technology Officer Council (GITOC): Standing Committee on Architecture.

Enquiries can be directed to:

The Chief Executive Officer
State Information Technology Agency (Pty) Ltd
459 Tsitsa Street, Erasmuskloof
PRETORIA, SOUTH AFRICA

The Chairperson
Government Information Technology Officer's Council
Department of Public Service and Administration
Batho Pele House, 116 Proes Street
PRETORIA, SOUTH AFRICA

This document is also available on the SITA website (<http://www.sita.co.za>)

COPYRIGHT, TRADEMARKS AND INTELLECTUAL PROPERTY

Some of the standards, acronyms and terms that are referenced in this publication are protected by copyright and/or intellectual property rights. The omission of the rightful copyright and/or intellectual property right owners' information from this document is merely intended to simplify the structure of the document.

This document, in part or in whole, may be freely used on condition that the source is quoted.

CONTENTS

1	OVERVIEW	6
1.1	INTRODUCTION	6
1.2	MANDATE	8
1.3	PURPOSE AND BENEFITS	8
1.4	SCOPE.....	9
1.4.1	Where does MIOS fit into the bigger picture?	9
1.4.2	What is included in MIOS?.....	9
1.4.3	What is excluded from MIOS?	10
1.5	APPLICABILITY AND COMPLIANCE	10
1.5.1	To whom does MIOS apply?	10
1.5.2	To what does MIOS apply?	10
1.5.3	Exemption from applicability.....	12
2	MANAGEMENT PROCESSES	13
2.1	PRINCIPLES	13
2.2	STANDARD SETTING.....	13
2.2.1	Standard Setting Responsibilities	13
2.2.2	Standard setting process	15
2.2.3	Standards Selection Principles.....	17
2.2.4	MIOS review frequency	17
2.3	STANDARDS CERTIFICATION.....	18
2.3.1	Standards Certification Responsibilities	18
2.3.2	Certification Process	20
3	MINIMUM INTEROPERABILITY STANDARDS (MIOS)	22
3.1	INTRODUCTION	22
3.2	STANDARDS DEVELOPMENT ORGANISATIONS	22
3.3	PUBLIC SECTOR AND COMMON DATA STANDARDS	24
3.4	TECHNICAL INTEROPERABILITY STANDARDS.....	28
	ANNEX A : ABBREVIATIONS.....	34
	ANNEX B : PARTICIPANTS.....	ERROR! BOOKMARK NOT DEFINED.
	ANNEX C : DOCUMENT HISTORY	ERROR! BOOKMARK NOT DEFINED.

FIGURES

Figure 1: Government ICT House of Value	6
Figure 2: e-Government information exchange scenarios	11
Figure 2: Standards selection and setting process.....	16
Figure 3: MIOS Certification Process.....	20
Figure 5: GWEA: Technology Reference Model (TRM)	28

1 OVERVIEW

1.1 INTRODUCTION

(1) The South African Government, as represented by its National, Provincial and Local departments and associated agencies, is committed to the continuous improvement of public service delivery. Such commitment has become an underlying theme across all departments' strategic and annual performance plans. Following on this commitment government ICT leaders have embarked on an e-Government programme in 2001, which aspires to achieve the effective, efficient and economic management and utilisation of Information and ICT Resources in government as illustrated in the Government ICT House of Value).

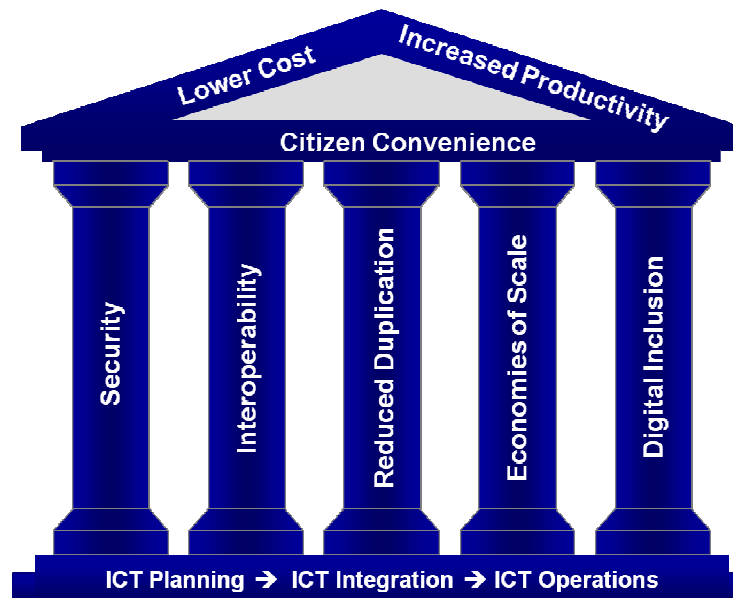


Figure 1: Government ICT House of Value

(2) The ICT House of Value serves as a reference to measure the performance of e-Government projects and systems, which includes interoperability¹. The strategic drive to advance the maturity on interoperability not only compels government ICT leaders to collaborate on e-Government initiatives by sharing scarce resources, but it also provides a way for information to be exchanged electronically across traditional government system boundaries in order to improve public service delivery.

(3) The ICT House of value, comprises a roof, pillars and foundation, each representing the following:

- (a) The **outcomes** (roof) of the e-Government programme on public sector operations are to:

¹ Interoperability (between information systems) means the ability of two or more information systems or technology components to interconnect and exchange data.

- (i) **Lower cost** of government service delivery operations, by reducing time, complexity, repetition and duplication of tasks.
 - (ii) **Increased productivity** of government operations, by improving the quality and quantity of traditional public sector outputs or introduce new processes to produce outputs and render services that were previously impossible.
 - (iii) **Citizen Convenience** when interacting with government, by offering equal access to government information systems and services, provides more and better information, improves information service quality and privacy, provides remedies for failures and offers best value for money².
- (b) The **value** (pillars) that the e-Government programme contributes to the public sector ICT environment is:
- (i) **Security**, by ensuring that information systems and related technologies operate in a maintained security environment.
 - (ii) **Interoperability**, by ensuring that information systems and ICT infrastructure of government can interconnect and exchange information.
 - (iii) **Reduced duplication**, by eliminating unnecessary duplications, by promoting sharing and consolidation of Information systems and ICT infrastructure across government.
 - (iv) **Economies of scale**, by leveraging collective purchasing power of government to lower unit prices from industry.
 - (v) **Digital inclusion**, by promoting the South African ICT industry, with a particular emphasis on Broad Based Black Economic Empowerment (BBBEE), labour absorption, and stimulation of equitable economic growth and skills development of ICT in South Africa.
- (c) The **capabilities** (foundation) by which to achieve the outcomes and values of e-Government are:
- (i) **ICT planning**, the capabilities that set direction and standards for ICT, Enterprise Architecture and to validate/certify conformance and performance thereto.
 - (ii) **ICT integration**, the capabilities that provide and develop ICT Systems and Technology Infrastructure into integrated ICT solutions.
 - (iii) **ICT operations**, the capabilities to ensure that ICT Systems and Technology Infrastructure are maintained in a reliable, available and secure environment.

(4) The advancement of interoperability in Government is an ongoing process and should be managed as a long-term programme. It is therefore incumbent upon the members of the Government Information Technology Officers Council to promote the objectives of interoperability and to observe the principles and comply with the standards as set out in MIOS during the life-cycle management of IS/ICT in government. It is also essential that MIOS remains updated and that it aligns to stakeholder requirements, changes in legislative

² "Batho Pele" (People First) principles for information oriented service delivery

environment, so that government can embrace the potential of technological advancement in the market and address the archival issues inherent to the digital age.

(5) The MIOS provides a set of mandatory standards that will ensure the achievement of the interoperability pillar in the ICT House of Value as illustrated in figure 1 above.

1.2 MANDATE

(1) Interoperability between Information Systems and Information-and-Communication Technology (IS/ICT) in government is mandated in accordance with the following legislation:

- (a) Public Service Act (Act 38 of 1994 as amended by Act 30 of 2007) mandates the Minister to establish norms and standards for Information Management in the Public Service and e-Government respectively;
- (b) Public Service Regulations 2001 (as amended 2001 to 2010) –
 - (i) Obliges heads of departments to comply with the MIOS.
 - (ii) Mandates the Minister to issue the MIOS.
 - (iii) Mandates the GITO Council to review and recommend to the Minister any amendments to the MIOS.
- (c) State Information Technology Agency (SITA) Act (Act 88 of 1998 as amended by Act 38 of 2002) sections 7(6)(a)(i) and 7(6)(b) mandates SITA to set standards for interoperability between information systems in government and to certify information technology goods and services for compliance against such standards.
- (d) State Information Technology Agency General Regulation (R.50 of 2005) sections 4.2 and 4.3 prescribe the processes to set interoperability standards and to certify compliance of information systems thereto.
- (e) Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) section 38(1)(b) and (d) holds an accounting officer responsible for the effective, efficient, economical and transparent use of the resources and to comply with audit commitments as required by legislation.

1.3 PURPOSE AND BENEFITS

(1) The *purpose* of the MIOS is to prescribe open system standards that will ensure minimum level of interoperability within and between IS/ICT systems that are utilised in government, industry, citizens and the international community in support of the e-Government objectives.

(2) The *benefits* that MIOS provides to stakeholders are:

- (a) To government IS/ICT management communities, it provides a framework to ensure compliance with interoperability stipulations as set out in the SITA Act and Public Service Regulations respectively. It further underpins the collective

value IS/ICT as a strategic resource of government that must be valued, shared and used to improve public service delivery.

- (b) To enterprise architects, solution architects, designers and implementers, it provides a basis for designing, using and implementing open standards based solutions to improve interoperability and reduce duplication across government IS/ICT.
- (c) To acquirers, it provides the minimum mandatory technical specifications that must form part of all bid documents.
- (d) To the Certification Authority, it serves as a baseline by which to verify and certify conformance of IS/ICT goods and services for use in government.
- (e) To SITA, it provides the technical standards that are required to function as the Prime Systems Integrator (PSI) for Government.
- (f) To ICT goods and service providers, it substantiates government's strategic intent towards the adoption of and migration to open standards and that only MIOS compliant products be considered for integration into the Government Information Infrastructure.

1.4 SCOPE

1.4.1 Where does MIOS fit into the bigger picture?

The MIOS is an integral part of the Government's envisaged IS/ICT Governance Framework. It is also strongly related to, although not part of, the Government Wide Enterprise Architecture (GWEA) Framework (which sets the minimum standard for developing ICT Plans and Blueprints in government), because the MIOS prescribes the architecture model and notation standards needed to achieve interoperability among Enterprise Architecture tools and repositories, and the GWEA Framework, in turn, prescribes the adherence to MIOS during the development of ICT Plans and Blueprints in government.

1.4.2 What is included in MIOS?

The Minimum Interoperability Standard (MIOS) contains the following:

- (a) The management processes and responsibilities for –
 - (i) the setting and approval of interoperability standards, and
 - (ii) the certification of IS/ICT products and services for compliance with such standards; and
- (b) The set of interoperability standards regarding –
 - (i) data format standards to enable exchange of data between government information systems (IS), and

- (ii) technical standards to interconnect, interoperate, access and exchange data among components of government Information and Communication Technology (ICT) infrastructure.

1.4.3 What is excluded from MIOS?

The MIOS **does not** prescribe any standards relating to business processes of IS/ICT services, except for the processes to set the standard and to certify compliance with such standards. The IS/ICT business process and service standards, such as ICT Governance practice standards, Enterprise Architecture practice standards, Information System Security practice standards, Quality Management practice standards, System Development Life Cycle (SDLC) practice standard, Project Management practice standard and ICT Service Management standards form part of the prevailing and evolving Government IS/ICT Governance Framework as referenced in par (1.4.1) above.

1.5 APPLICABILITY AND COMPLIANCE

1.5.1 To whom does MIOS apply?

The MIOS is normative – it is prescriptive and compliance is mandatory – to heads of National and Provincial departments and associated agencies/entities as listed in the Schedules to the Public Service Act, and it is informative – it is descriptive and compliance is not mandatory – to heads of Local Government.

1.5.2 To what does MIOS apply?

- (1) According to the Public Service Regulation, Chapter 5 (e-Government), Part III, C –

“C.1 The following systems shall comply with the MIOS:

(a) every part of any new information system developed or acquired for the public service or any upgrade of any existing information system in the public service; and

(b) every legacy system that is part of electronic service delivery in the public service.

C.2 A head of department shall include compliance with the MIOS in the project approval procedure for the department. The MIOS shall be used in the audit and review of every project of a department.”

- (2) In context of e-Government, MIOS is applicable for compliance to all e-Government systems through their life-cycle of existence, where:

- (a) e-Government system means “any information system in the public service” and the interoperability of e-Government systems (as illustrated in Figure 2: e-Government information exchange scenarios), is described as –

- (i) **Government to Government (G2G) information system** – any government information system that interconnects and exchanges information with another government information system (including any two information systems within a department).
- (ii) **Government to Business (G2B) information system** – any government information system that interconnects and exchanges information with a commercial or non-governmental business entity; and
- (iii) **Government to Citizen (G2C) system** – any government information system that interconnects and exchanges information with a citizen or community.

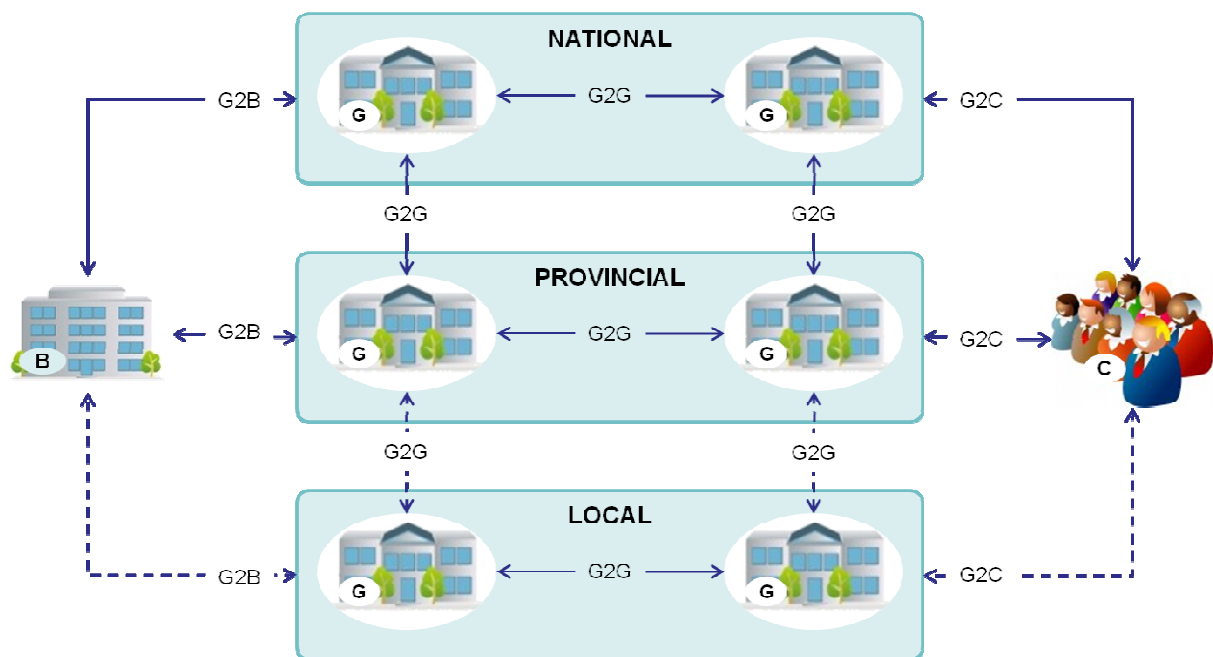


Figure 2: e-Government information exchange scenarios

- (b) The life-cycle stages and conditions when MIOS is applicable, are for –
 - (i) A new e-Government system that is either under development or in acquisition;
 - (ii) An e-Government system that is upgraded in functionality to enable new business processes or that is upgraded in terms of its technology infrastructure (i.e. same business processes and functionality, but new technology infrastructure)
 - (iii) An existing (legacy) e-Government system in operation.

1.5.3 Exemption from applicability

- (1) A department or agency may apply to the Minister to be exempted from complying with MIOS.
- (2) The MIOS is recommended for, and will not be subjected to compliance certification, for information systems that are –
 - (a) Specific to the unique operational requirements of a Department or Agency, provided that such a system is not an e-Government system; or
 - (b) Governed by strict international health or safety standards; or
 - (c) Embedded systems or closed systems (such as electro-mechanical systems, closed surveillance systems and real-time monitoring systems) that does not interoperate or exchange data with another system.

2 MANAGEMENT PROCESSES

2.1 PRINCIPLES

In addition to the legislation on IS/ICT in government, the following principles regarding MIOS serve as a basis for decision-making:

- (a) Approval of funding for the acquisition (including the development) of new or the modification of existing IS/ICT products or systems are dependant on the IS/ICT product or system being compliant with MIOS.
- (b) In terms of the Public Finance Management Act (PFMA) it is the responsibility of the accounting officer of a department or agency to ensure that IS/ICT projects and system comply with MIOS and that such compliance is subject to be audited/verified by the Auditor-general.
- (c) When interconnectivity, data interoperability or information access is required between departments' or agencies' systems, the cost of rectifying a system that does not comply with MIOS rests with the owner of the non-compliant product or system.

2.2 STANDARD SETTING

2.2.1 Standard Setting Responsibilities

(1) The responsibilities and process for setting interoperability standards are governed in terms of the following legislation –

- (a) Public Service Act states:
*“3. (1) The Minister [of Public Service and Administration] is responsible for establishing norms and standards relating to – ...
(f) information management in the public service;
(g) electronic government;”*
- (b) Public Service Regulations, Chapter 5, Part III, states:
*“B. MINIMUM INTEROPERABILITY STANDARDS
B.1 The Minister shall, after consultation with the Government Information Technology Officer Council (herein referred to as the “GITO Council”), issue Minimum Interoperability Standards (herein referred to as the “MIOS”) ...
D. REVIEW OF MIOS
For the purpose of recommending to the Minister new standards or the amendment or repeal of existing standards, the GITO Council shall from time to time review the MIOS.”*

(c) SITA Act, states:

“7(6) The Agency –

(a) must set standards regarding –

(i) the interoperability of information systems subject to the approval of the Minister;

(b) must certify every acquisition of any information technology goods or services by a department for compliance with those standards.”

(d) SITA General Regulations, states:

“4.2 SETTING OF STANDARDS

4.2.1 Before setting or amending standards regarding the interoperability of information systems between departments ... in terms of section 7(6)(a) of the Act, the Agency must -

(a) consult with departments and the GITO Council in order to assess the status of implemented systems and the proposed requirements;

(b) conduct an implementation impact analysis and develop a business case demonstrating the cost-effectiveness of such standards; and

(c) give due consideration to all representations received from departments and the GITO Council before submitting proposed standards, or an amendment thereof, to the Minister ... for approval

4.2.2 The Agency must set the standards, contemplated in section 7(6)(a) of the [SITA] Act, not later than a date determined by the Minister.”

4.2.3 The standards set in terms of section 7(6)(a) of the [SITA] Act must be made available to all heads of departments and on the Agency's web site.”

(2) Following above legislation, the stakeholders and their respective responsibilities regarding the setting of interoperability standards are –

No	Stakeholder	Role and Responsibilities
1	Minister of Public Service and Administration (MPSA)	The standards promulgation authority to – a) Approve and issue the MIOS for implementation.
2	State Information Technology Agency (SITA)	The standards setting authority to – a) Consult with and consider inputs from departments and GITO Council and keep abreast of standards development in the ICT industry. b) Conduct implementation impact analysis of changes to MIOS. c) Select and set the standards in MIOS. d) Manage the development, configuration and dissemination of the MIOS. e) Submit MIOS to GITOC for recommendation to

No	Stakeholder	Role and Responsibilities
		Minister.
3	GITO Council	The standards recommending authority to – a) Initiate the review of the MIOS. b) Give direction to the working group in 4 below and monitor amendments to MIOS. c) Recommend the MIOS to the Minister for approval.
4	GITO Council Standing Committee on Architecture (SCARC)	The standards working group, delegated by the GITO Council, to – a) Promote the advancement of interoperability. b) Collaborate, improve and resolve technical issues on MIOS improvement. c) Assess the risk and impact of changes to the MIOS on e-Government systems.

2.2.2 Standard setting process

(1) The task of advancing interoperability between information systems across the public sector is a complex and on-going process. The interoperability standards, as contained in MIOS, must support and enhance Government's business processes, and also ensure that new technological advances and innovations are leveraged to their full advantage.

(2) The process to review and set interoperability standards is inclusive. Therefore, all stakeholders, including Government Departments and their agencies, industry and the users are all encouraged to participate in improving interoperability, and to provide support on the implementation of the MIOS.

(3) The process to review and set interoperability standards for inclusion in MIOS is a consultative decision-making process that comprises a few steps involving a rule based filtration of interoperability standards as illustrated in Figure 3: Standards selection and setting process, and described as follows –

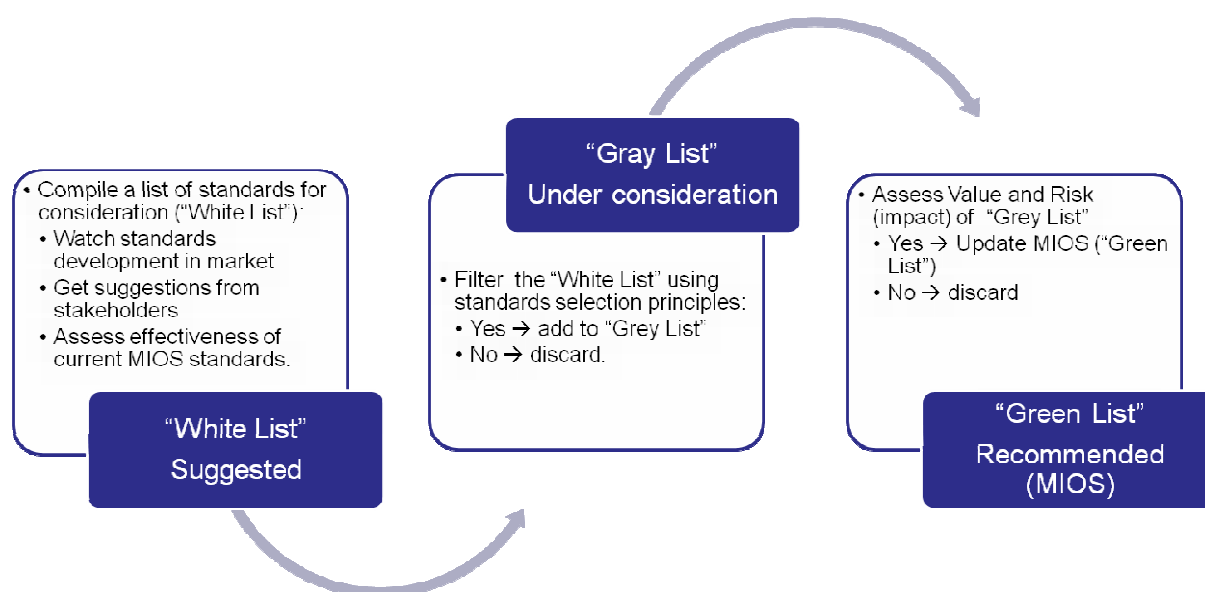


Figure 3: Standards selection and setting process

- (a) **Step1:** Compile a list of standards for consideration – referred to as the “White List”. The White List is an unbounded (unscreened) list of new or revised interoperability standards that are suggested by all stakeholders to be considered by the standards setting task team for inclusion into MIOS. This list is compiled by means of the following activities –
- Watch or keep abreast of standards development in the ICT market that involves periodic research into national and international standards development organisations and exploring the developments of other governments’ e-Government and interoperability programmes.
 - Consult with and solicit inputs from government stakeholders and interoperability champions.
 - Assess the effectiveness and relevance of the interoperability standards that are contained in the existing MIOS to identify standards that are not contributing (anymore) to the advancement of interoperability in government.
- (b) **Step 2:** Filter the “White List” using the standards selection principles (as contained in section 2.2.3 below) and produce a list of candidate standards – referred to as the “Grey List”. The standards setting task team considers each standard in the White List and test it for conformance with the standard selection principles –
- A conformant standard is placed in the “Grey List”, which will be considered, subject to a further evaluation, for inclusion into MIOS.

- (ii) A non-conformant standard is discarded, and will not be considered for further evaluation.
- (c) **Step 3:** Assess the value and risks of standards in the “Grey List” and produce a list of recommended standards that will be added to or supersede existing standards in the MIOS – referred to as the “Green List”. The standards setting task team considers each standard in the Grey List and perform a benefit-risk impact assessment –
 - (i) A standard that passes the benefit-risk impact assessment is placed on the “Green List” and will be added to or supersede existing standards in the MIOS.
 - (ii) A standard that fails the benefit-risk impact assessment will be discarded and flagged as deprecated. A deprecated standard does not contribute to the advancement of interoperability in government anymore or it will introduce an unacceptable high risk to the public service delivery.

2.2.3 Standards Selection Principles

The following principles shall apply during the selection of interoperability standards for inclusion or amendment to the MIOS:

- (a) **Interoperability:** The standard is designed to advance interconnectedness and data exchange within and between e-Government systems.
- (b) **Openness:** the specifications for the standards is open, which is characterised by:
 - (i) The standard should be maintained by a non-commercial organization.
 - (ii) The standard development and decision-making processes are inclusive and open to all interested parties.
 - (iii) The standards development outputs, including documents, drafts and completed standards, are accessible to anyone at no cost or at a negligible fee.
 - (iv) The intellectual rights required to implement the standard (e.g. essential patent claims) are irrevocably available, without any royalties attached.
 - (v) The standard must not favour or provide exclusive rights to a particular vendor or product brand.
- (c) **Industry support:** the standard is widely supported by the industry, and is likely to reduce the cost of and the risk inherent to e-Government systems.

2.2.4 MIOS review frequency

- (1) The MIOS should be reviewed and updated on a bi-annual basis (once every two years), unless determined otherwise by the Minister. This review will be known as a major version update. (Note: The latest approved version of MIOS will remain in effect until it is superseded)
- (2) Due to the rapid advancement of technology and associated proliferation of standards, it may be necessary to review parts of the MIOS from time to time to incorporate such

advancements and changes of IS/ICT in government and industry. This review will be known as the minor version update.

2.3 STANDARDS CERTIFICATION

2.3.1 Standards Certification Responsibilities

(1) Standards Certification is a process that verifies whether an e-Government system complies with the standards that are contained in MIOS. The responsibility to certify that e-Government systems comply with the MIOS are governed in terms of the following legislation:

- (a) Public Service Regulations, Chapter 5, Part III, C states:

“C.2 A head of department shall include compliance with the MIOS in the project approval procedure for the department. The MIOS shall be used in the audit and review of every project of a department.”

- (b) SITA Act, states:

“7(6) The Agency ... (b) must certify every acquisition of any information technology goods or services by a department for compliance with those standards.”

- (c) SITA General Regulations, states:

“4.3 CERTIFICATION OF INFORMATION TECHNOLOGY GOODS AND SERVICES

4.3.1 The Agency must, ..., conduct standard certification in respect of all information technology goods or services, which were acquired by departments before the commencement of these Regulations. ...

4.3.3 The Agency must conduct standard certification of information technology goods or services –

(a) acquired ... by a department from the Agency; ... and

(b) procured ... by a department through the Agency ...”

(2) From the above legislation, the stakeholders and their respective responsibilities regarding standards certification are as follows:

No	Stakeholder	Role and Responsibilities
1	Head of Department	The Accounting officer, who must ensure and account/report that all e-Government systems (assets) under his/her control comply with the MIOS.
2	SITA	The Certification Authority, who must certify that all e-Government systems – in acquisition and in operation – comply with MIOS.
3	Supplier / ICT Industry	Supplier, Provider and/or Integrator of e-Government systems, who must provide evidence that the

No	Stakeholder	Role and Responsibilities
		e-Government system comply with MIOS.

2.3.2 Certification Process

- (1) All e-Government systems must comply with MIOS. The certification management process implements the necessary controls into the existing Supply Chain Management, Solution Development and Solution Integration processes in order to meet the legislative requirement on interoperability.
- (2) The certification controls are illustrated in Figure 4: MIOS Certification Process and is described in the following table: (Note: The illustration is not intended to describe the requirements management, supply chain, solution development or solution integration processes of government.)

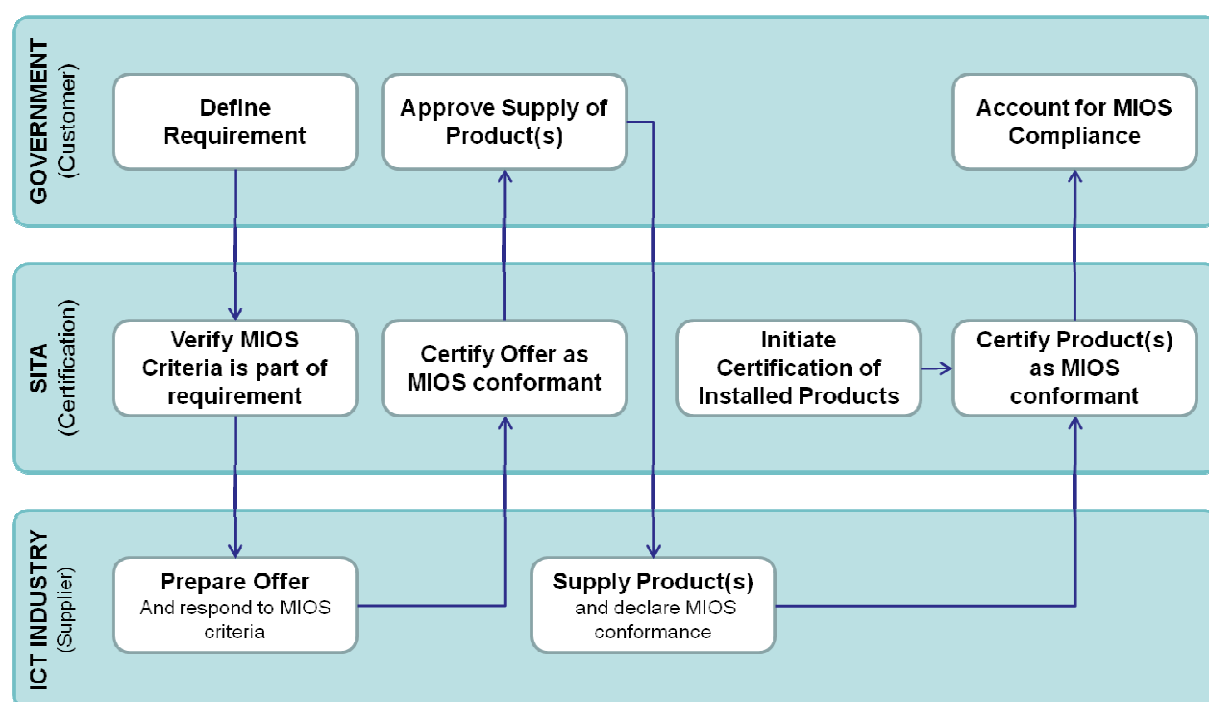


Figure 4: MIOS Certification Process

No	Step	Responsibility and Activities
1	Define Requirement	Government (customer) defines the requirement for the acquisition or renewal of an e-Government System, which include the functional and technical requirements; and submit same to SITA Certification.
2	Verify MIOS criteria is part of requirement	SITA Certification verifies that the requirement (i.e. technical specification) includes the relevant MIOS Conformance Criteria as part of the Mandatory Technical Specifications in the Bid Document. This will inform prospective bidders/suppliers that their product on offer will be subject to MIOS Certification.

No	Step	Responsibility and Activities
		Note: Any conflicting technical specification (between the customer specification and the MIOS criteria) will be resolved before the request for bid documentation is published to prospective suppliers.
3	Prepare Offer	The prospective suppliers of ICT products prepare their offers and are obliged to indicate conformance of their product(s) to the MIOS criteria.
4	Certify Offer as MIOS Conformant	SITA Certification evaluates and verifies that the specifications of the product as offered by suppliers are conformant to the MIOS criteria, and issue a <u>“MIOS Offer Certificate of Conformance”</u> based on the offer.
5	Approve Supply of Product(s)	The customer verifies that the offer(s) meets his/her requirements and that it conforms to MIOS, and approves that the supply of the product(s) may proceed.
6a	Supply Product(s)	The supplier supplies the product(s) and declares with evidence that the actual product(s) conform to MIOS criteria.
6b	Initiate Certification of Installed Product(s)	SITA Certification may also on behalf of a department initiate a process or project to certify that legacy (installed) e-Government systems conform to MIOS.
7	Certify product(s) as MIOS conformant	SITA Certification unit evaluates and tests the actual installed product(s) – new or legacy product(s) – based on hard evidence by the supplier or interoperability test results or both and issues a <u>“MIOS Product Certificate of Conformance”</u> . (A Certificate is issued per product)
8	Account for MIOS compliance	The Customer reports to the designated executive authority and give account to the Auditor General that his/her department comply with MIOS as legislated.

3 MINIMUM INTEROPERABILITY STANDARDS (MIOS)

3.1 INTRODUCTION

(1) This section of the MIOS defines the minimum set of open standards that are necessary to achieve the minimum level of interoperability across e-Government systems, and cites the standards development organisations from where these standards can be obtained.

(2) The list of interoperability standards is divided into two sections:

- (a) **Public Sector Records and Data Standards**, which must be used to achieve interoperability (data exchange) among e-Government information systems (IS); and
- (b) **Technical Interoperability Standards**, which must be used to achieve the required level of interoperability (i.e. network connectivity, data exchange protocols and interfaces, and uniform data access and presentation) across government ICT infrastructure.

The following convention is used in the respective standards tables:

- “Ref” = Unique MIOS Reference Number of the standard.
- “Provider” means the Standards Development Organisation (SDO) who is either the owner or custodian of the interoperability standard as the case may be.
- Text in square brackets [] denotes the Standard Reference Number as allocated by the SDO.
- Text in braces / curly brackets {} denotes a guideline or constraint on the implementation of the standard.

3.2 STANDARDS DEVELOPMENT ORGANISATIONS

The following Standards Development Organisations (SDOs) are cited in the MIOS. SDOs marked with an asterisk (*) indicate that the standards are available from their respective web sites (Uniform Resource Locators (URL)).

<i>SDO</i>	<i>Description</i>	<i>Uniform Resource Locator (URL)</i>
ADL *	Advanced Distributed Learning	http://www.adlnet.gov
ANSI	American National Standards Institute	http://www.ansi.org
DHA	Department of Home Affairs (South Africa)	http://www.dha.gov.za
DSD	Department of Social Development (South Africa)	http://www.dsd.gov.za

SDO	Description	Uniform Resource Locator (URL)
ECMA	Ecma International - European association for standardizing information and communication systems (formerly known as "European Computer Manufacturers Association")	http://www.ecma-international.org
ETSI	European Telecommunications Standard Institute	http://www.etsi.org
NIST	National Institute of Standards and Technology [USA]: Federal Information Processing Standards	http://www.itl.nist.gov/fipspubs
IEEE	Institute of Electrical and Electronics Engineers	http://www.ieee.org
IETF *	Internet Engineering Task Force	http://www.ietf.org
IJS	Integrated Justice System	http://www.ijs.gov.za
ISO	International Organisation for Standardization	http://www.iso.org
ITU	International Telecommunication Union	http://www.itu.int
OAI *	Open Archives Initiative	http://www.openarchives.org
OASIS *	Organization for the Advancement of Structured Information Standards	http://www.oasis-open.org
OCLC	Online Computer Library Center	http://www.oclc.org
OGC *	Open Geospatial Consortium	http://www.opengeospatial.org
OMA	Open Mobile Alliance	http://www.openmobilealliance.org
OMG *	Object Management Group®	http://www.omg.org
PKWARE	PKWARE® Inc, open standard for compressed file format, ZIP)	http://www.pkware.com
SABS	South African Bureau of Standards (SDO for South African National Standards (SANS))	http://www.sabs.co.za
SITA *	State Information Technology Agency	http://www.sita.co.za http://www.ifms.gov.za
W3C *	World Wide Web Consortium	http://www.w3c.org
WHO *	World Health Organisation	http://www.who.int

3.3 PUBLIC SECTOR SPECIFIC AND COMMON DATA STANDARDS

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard and Identifier</i>	<i>Provider</i>
D-1	Governance and Administration data standards		
D-1.1	Administration Records	<p>Integrated Finance Management System (IFMS) Canonical Information Model (CIM): Financial Management, Supply Chain Management and Human Resource Management.</p> <p>{IFMS CIM is under development and is intended to supersede all existing Financial, Supply Chain and Human Resource data interchange standards for the Public Service; and it is not applicable to legacy systems}</p>	SITA (IFMS)
D-2	Identification and Citizen Status data standards		
D-2.1	Citizen Status Record	<p>Citizen Status Record Definition (as per National Population Register (NPR))</p> <p>{NPR contains information of South African citizens, permanent residents and refugees who is identified by a unique Identity (ID) Number, Birth, Death, Marriage status, emigration or immigration status, passports and identity documents information.}</p>	DHA
D-2.2	Biometric Data Element Specification	[SANS 19785-1]: Information Technology – Common Biometric Exchange Formats Framework – Part 1: Data Element specification	SABS
D-2.3	Biometric Data Interchange	[SANS 19794]: Information Technology Biometric data interchange formats – Part 1: Framework, Part 2: Finger minutiae data, Part 3: Finger pattern spectral, Part 4: Finger image data, Part 5: Face image data, and Part 7: Signature/sign behaviour.	SABS
D-3	Health data standards		
D-3.1	Disease codes	International Statistical Classification of Diseases and Related Health Problems, 10th Revision (ICD-10)	WHO

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard and Identifier</i>	<i>Provider</i>
D-3.2	Health Image records	Digital Imaging and Communications in Medicine (DICOM), [ISO/IEC 12052]	ISO
D-4	Social data standards		
D-4.1	Child Protection Records	<ul style="list-style-type: none"> Child Protection Register data schema (Part A and B: Core Data schema and Data schema to support Integrated Justice System (IJS)) Child In Need of Care and Protection data schema Child Adoption Data schema Child Abduction Data schema Child Trafficked Data schema 	DSD
D-4.2	Non-Profit Organisation Records	Non-Profit Organisation Register Data schema	DSD
D-4.3	Child In Conflict With The Law Records	<ul style="list-style-type: none"> Child Youth Care Data schema Secure Care Detention Facility Management (IAS) Data schema Child Justice Forms: Data schema 	DSD
D-5	Justice data standards		
D-5.1	Criminal Justice records	<p>South African Justice XML (SAJXML) Schema v1.3.0</p> <p>{The SAJXML schema is under development and is subject to change.}</p>	IJS
D-6	Education and Learning data standards		
D-6.1	Learner Unit Records	Learner Unit Record Information Tracking System (LURITS), Data Interchange standard, Version 1.3, March 2010	SITA
D-6.2	e-Learning/ Learning Management System	Sharable Content Object Reference Model (SCORM) v1.2, Oct 2001	ADL
D-7	Geographic and Location data standards		
D-7.1	Cadastre and Addressing	Geographic Information – Address Standard, Part 1: Data format of addresses [SANS 1883-1]	SABS
D-7.2	Geospatial data	Geospatial Markup Language (GML) [ISO/IEC 19136:2007]	OGC and ISO
D-8	Common Data standards		
D-8.1	Hypertext Markup Language	<ul style="list-style-type: none"> Hypertext Markup Language (HTML) v4.01 	W3C

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard and Identifier</i>	<i>Provider</i>
		<ul style="list-style-type: none"> eXtensible Hypertext Markup Language (XHTML) v1.0 (Second Edition) <p>{Government information systems will be designed so that as much information as possible can be accessed and manipulated from common commercial browsers through utilisation of functionality that is freely supported and available within the browser community. Refer also to MIOS T-5.13 Web Content Accessibility Guideline}</p>	
D-8.2	Wireless Hypertext Markup Language	Wireless Application Protocol (WAP) v2.0	OMA
D-8.3	Extensible Markup Language Syntax	<p>Extensible Markup Language (XML) Version 1.0 (Fifth Edition)</p> <p>{Avoid the use of any product specific XML extensions that are not being considered for open standardisation within the W3C.}</p>	W3C
D-8.4	Extensible Markup Language Schema	<ul style="list-style-type: none"> XML Schema Part 1: Structures Second Edition; and XML Schema Part 2: Data types Second Edition; OR REGular LAnguage for XML Next Generation (RelaxNG), [ISO/IEC 19757] 	W3C OASIS/ISO
D-8.5	Character set	<ul style="list-style-type: none"> Transformation Format – 8 bit UTF-8/ASCII Formatted Text [RFC 3629] UNICODE [ISO/IEC 10646-1:2000] 	IETF ISO
D-8.6	e-Mail message format	Multipurpose Internet Mail Extensions, MIME [RFC 2045, 2046, 2047, 2048 and 2077]	IETF
D-8.7	Office Document formats	<ul style="list-style-type: none"> Open Document Format (ODF) v1.0 [SANS 26300] Comma-Separated Values (CSV) [RFC4180] <p>{for use in word-processing, spreadsheet, and presentation office suites}</p>	SABS IETF
D-8.8	Portable Document Format	Document management – Portable document format – Part 1: PDF 1.7 [SANS 32000-1]	SABS

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard and Identifier</i>	<i>Provider</i>
		{for use in publishing and distributing read-only, preformatted forms and non-editable portable documents}	
D-8.9	Graphical/still image file format	<ul style="list-style-type: none"> ▪ Joint Photographic Experts Group (JPEG) [ISO/IEC 10918-1:1994 Digital compression and coding of continuous-tone still images] ▪ Portable Network Graphics (PNG) [ISO/IEC 15948:2004] ▪ Tagged Image File Format (TIFF) v6 <p>{TIFF should only be used for images that does not tolerate information loss}</p>	ISO ISO Adobe
D-8.10	Multimedia audio/visual format	<ul style="list-style-type: none"> ▪ Moving Picture Experts Group 1 (MPEG-1), including MPEG-1 Audio Layer III (MP3), [ISO/IEC 11172] ▪ Moving Picture Expert Group 2 (MPEG-2), [SANS 13818] ▪ MPEG-4 Part 10, Advanced Video Coding / H.264 (ISO/IEC 14496-10) 	ISO SABS ISO
D-8.11	Compressed file format	<ul style="list-style-type: none"> ▪ Tape Archive (tar) [POSIX.1-2001] using GNU zip (gzip) [RFC1951 and RFC1952] or bzip2 ▪ ZIP [APPNOTE.TXT - .ZIP File Format Specification Version: 6.3.2 (2007)] 	POSIX IETF PKWARE

3.4 TECHNICAL INTEROPERABILITY STANDARDS

(1) The Technical Interoperability Standards are grouped in accordance with the Government Wide Enterprise Architecture Framework: Technology Reference Model as illustrated in Figure 5: GWEA: Technology Reference Model (TRM)

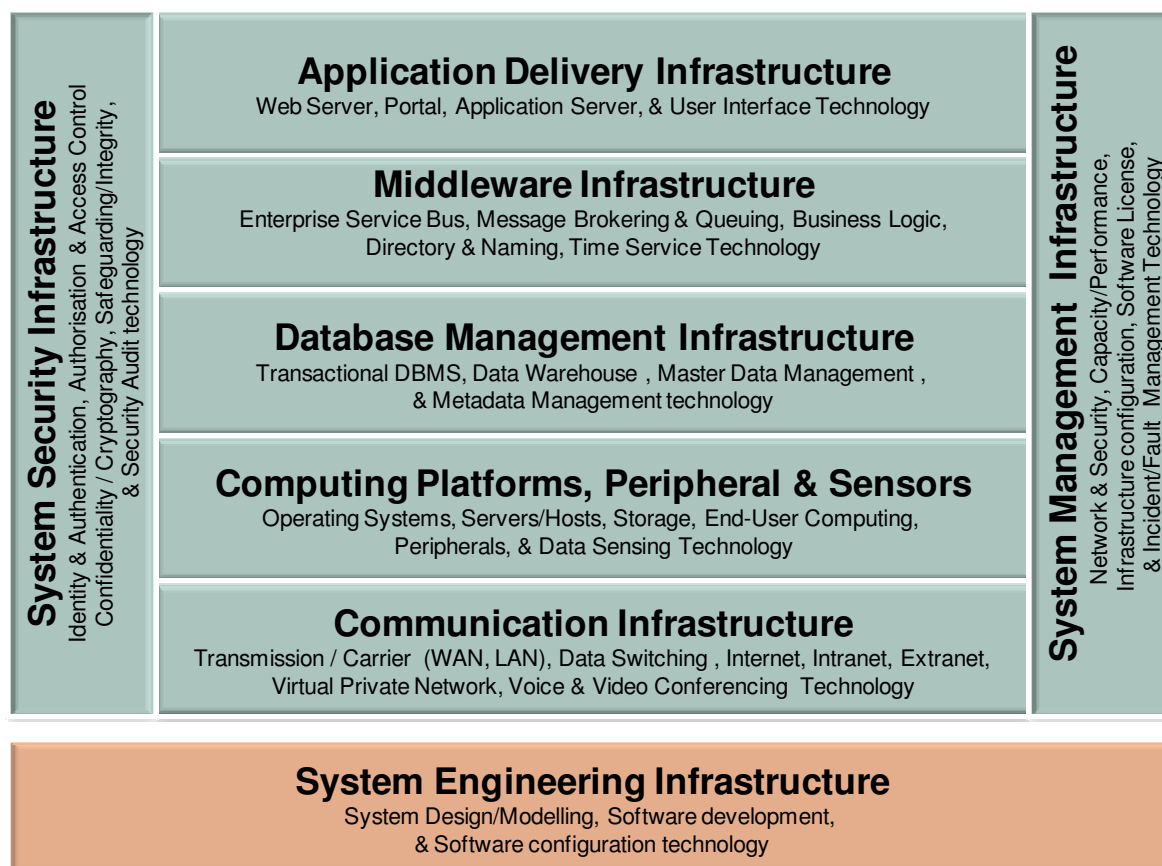


Figure 5: GWEA: Technology Reference Model (TRM)

Ref	Component	Interoperability Standard	SDO
T-1	Communications Infrastructure		
T-1.1	LAN/WAN interworking	<ul style="list-style-type: none"> Internet Protocol (IP) Version 4 [RFC 791]; and Transmission Control Protocol (TCP) [RFC 793, RFC 4614]; and User Datagram Protocol (UDP) [RFC 768]. <p>{Government organisations are to interconnect using TCP/IP v4, and noting that RSA Government is considering the adoption of IPv6 in due course. Peering agreements should be investigated and considered where possible}</p>	IETF

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard</i>	<i>SDO</i>
T-1.2	LAN/WAN Internet Conferencing	Audiovisual and multimedia systems, [H.323] Session Initiation Protocol (SIP), [RFC 3261]	ITU IETF
T-1.3	Mobile Data link	The General Packet Radio Service (GPRS) specifications for Mobile Stations ("2G"), [EN No: 310 113, 301 344, 301 347 and TS 101 297, 101 351]	ETSI
T-1.4	Mobile Text Message	The Short Message Service (SMS) specifications for Mobile Stations including, [ETS 300 536 & 537, 300 559 & 560]	ETSI
T-1.5	Mobile Multimedia Message	The Multimedia Messaging Service (MMS) specifications for Mobile Stations, [TS 122 140, 123 140, 126 140]	ETSI
T-2	Computing Platforms, Peripherals and Sensors		
T-2.1		{No prescribed minimum interoperability standards}	
T-3	Database Management Infrastructure		
T-3.1	Relational Database Query Language	Structured Query Language (SQL) 2006, [ISO/IEC 9075-14:2006]	ISO/IEC
T-3.2	Content management metadata	Information and documentation - The Dublin Core metadata element set [SANS 15836]	SABS
T-3.3	Metadata harvesting	Open Archives Initiative Protocol for Metadata Harvesting 2.0 (OAI-PMH), [T20:42:00Z]	OAI
T-3.4	Ontology-based information exchange	Web Ontology Language (OWL) Semantics and Abstract Syntax	W3C
T-3.5	Content-sensitive linking	OpenURL v1.0 [ANSI/NISO Z38.88-2004] {The openURL is designed to enable the transfer of the metadata from the information service to a service component that can provide context- sensitive services for the transferred metadata}	ANSI
T-4	Middleware Infrastructure		
T-4.1	Directory schema	X.500 core schema [ISO/IEC 9594].	IEC/ISO
T-4.2	Directory access	Lightweight Directory Access Protocol LDAP v3 [RFC 4510]	IETF

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard</i>	<i>SDO</i>
		{For use in general-purpose directory user access}	
T-4.3	Internet domain naming	Domain Name System (DNS) [RFC 1032 to RFC1035 and related updates] {Projects are to follow the South African Government Domain Naming policy. Domain Name Services (DNS) must be used for Internet and Intranet IP address name resolution.}	IETF
T-4.4	Web service access	Simple Object Access Protocol SOAP v1.2 (Second Edition)	W3C
T-4.5	Web service registry	Universal Description, Discovery and Integration UDDI v3.0	OASIS
T-4.6	Web service description	Web Service Description Language (WSDL) v2.0	W3C
T-5	Application Delivery Services and Information Access		
T-5.1	Web transport	Hypertext Transfer Protocol, HTTP v1.1 [RFC 2616]	IETF/W3C
T-5.2	Web forms	Xforms v1.1 (2009)	W3C
T-5.3	Browser scripting	JavaScript [ECMA 262]	ECMA
T-5.4	e-Mail transport	Simple Mail Transfer Protocol SMTP [RFC 2821, RFC 2822]	IETF
T-5.5	e-Mail access	<ul style="list-style-type: none"> Internet Message Access Protocol v4 Rel 1, IMAP v4.1 [RFC 3501] or Post Office Protocol version 3, POP3 [RFC 1939] 	IETF
T-5.6	Internet File transfer	<ul style="list-style-type: none"> File Transfer Protocol (FTP), [RFC 959, RFC 1579, RFC 2428] Secure copy (SCP) [OpenBSD reference implementation] {Restart and recovery functionality of FTP are to be used when transferring very large files}	IETF
T-5.7	XML Data transformation	Extensible Stylesheet Language (XSL) v1.1	W3C
T-5.8	XML Data query	XML Path Language (XPath) v2.0	W3C
T-5.9	XML Signature	<ul style="list-style-type: none"> XML Signature Syntax and Processing (Second Edition) XML Digital Signatures (XML-DSIG) in the 2006 XML Environment 	W3C
T-5.10	Digital Object Identification	Syntax for the Digital Object Identifier [ANSI z39.84] {for use in digital rights management}	ANSI

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard</i>	<i>SDO</i>
T-5.11	Web Content syndication	<ul style="list-style-type: none"> Resource Description Framework (RDF) Site Summary (RSS) Version 1.0, [RSS-DEV working Group, http://web.resource.org] Really Simple Syndication (RSS) Version 2.0, [RSS 2.0, Berkman Center at Harvard Law School, http://cyber.law.harvard.edu/rss/] 	
T-5.12	Distributed searching and Retrieval	<ul style="list-style-type: none"> Information Retrieval: Application Service Definition and Protocol Specification, Z39.50 [ANSI/NISO Z39.50, ISO/IEC 23950:1998] Search Retrieval via URL (SRU) Version 1.2 [http://www.loc.gov/standards/sru/] 	ANSI
T-5.13	Web Accessibility for the visual impaired	<p>Web Content Accessibility Guidelines (WCAG) 2.0 (2008)</p> <p>{A guideline for development of government websites and/or web enabled applications to improve access for the visual impaired user community}</p>	W3C
T-6	System Security		
T-6.1	E-Mail Security	<p>Secure/Multipurpose Internet Mail Extensions (S/MIME) V3 [RFC 2630 to RFC 2633]</p> <p>{shall be used where appropriate for pan government messaging security unless security requirements dictate otherwise}.</p>	IETF
T-6.2	IP Network security and Virtual Private Networking	Security Architecture for the Internet Protocol (Internet Protocol Security (IPsec)) , [RFC 4301]	IETF
T-6.3	IP Network authentication and encapsulation security	<ul style="list-style-type: none"> IP Authentication Header (AH) [RFC 4302], and IP Encapsulating Security Payload (ESP), [RFC 4303] 	IETF
T-6.4	Transport Layer security	Transport Layer Security (TLS) Protocol Version 1.2, [RFC 5246]	IETF
T-6.5	Encryption algorithms (block and stream ciphers)	<ul style="list-style-type: none"> Advanced Encryption Standard (AES), [SANS18033-3 Information technology - Security techniques - Encryption algorithms Part 3: Block ciphers]; OR TWOFISH, [FIPS PUB 197] <p>{AES is the preferred cipher algorithm and it should</p>	<p>SABS</p> <p>NIST</p>

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard</i>	<i>SDO</i>
		be used for both block and stream ciphers applications. TWOFISH should only be used as an alternative where AES is not possible.}	
T-6.6	Encryption algorithms (asymmetric ciphers)	<ul style="list-style-type: none"> ▪ RSA 2048bit (Rivest, Shamir and Adleman), [SANS 18033-2 Security techniques - Encryption algorithms Part 2: Asymmetric ciphers]; Or ▪ ECC 256 bit (Elliptic Curve Cryptography), [SANS 15946 Security techniques - Cryptographic techniques based on elliptic curves] 	SABS
T-6.7	Hashing	Secure Hash Algorithm II (SHA-II) SHA-256, or SHA-384 [SANS 18033 -3 or ISO/IEC 10118-3]	SABS
T-6.8	Message Authentication	<ul style="list-style-type: none"> ▪ Message Authentication Code (MAC) with Block cipher [SANS 9797-1]; and/or ▪ Message Authentication Code (MAC) with Hash function [SANS 9797-2] 	SABS
T-6.9	Digital Signatures	<ul style="list-style-type: none"> ▪ <u>RSA-DSA (Rivest, Shamir and Adleman - Digital Signing Algorithm) [SANS 14888]; or</u> ▪ <u>EC-DSA (Elyptic Curve - Digital Signing Algorithm, [SANS 14888]</u> 	SABS
T-6.10	Key Management	Security Techniques - Key Management: Part 3 Mechanisms using asymmetric techniques [SANS 11770-3:2009]	SABS
T-6.11	Public Key Infrastructure certificates	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (X.509 v3), [RFC 5280]	ITU
T-6.12	XML Security mark-up	Security Assertion Markup Language (SAML) v2.0	OASIS
T-6.13	Secure XML Encoding for exchanging biometric data	OASIS XCBF 1.1 Specification. Secure XML encodings for the patron formats specified in CBEFF, the Common Biometric Exchange File Format [NISTIR 6529].	OASIS
T-7	System Management		
T-7.1	Network Management Protocol	Simple Network Management Protocol (SNMP) v3 [RFC 3411-RFC 3418]	IETF
T-8	System Engineering		
T-8.1	Software	Unified Modelling Language (UML) v2.1.1	OMG

<i>Ref</i>	<i>Component</i>	<i>Interoperability Standard</i>	<i>SDO</i>
	Engineering Modelling Language		
T-8.2	Business Process Modelling Language	Business Process Model and Notation (BPMN) v1.1	OMG
T-8.3	Business Function Modelling Language	Integrated Definition Language for Function Modelling (IDEF-0) – Federal Information Processing Standard Publication 183, [FIPS PUB 183]	NIST
T-8.4	Model exchange	XML Metadata Interchange (XMI) version 2.1	OMG

Annex A : ABBREVIATIONS

BBBEE	Broad Based Black Economic Empowerment
BPMN	Business Process Modelling Notation
EA	Enterprise Architecture
GITO	Government Information Technology Officer
GITOC	Government Information Technology Officers Council
GWEA	Government Wide Enterprise Architecture
ICT	Information and Communication Technology
ISO	International Organisation for Standardisation
MIOS	Minimum Interoperability Standards
SCARC	Standing Committee on Architecture
SITA	State Information Technology Agency
OMG	Object Management Group
TOGAF®	The Open Group Architecture Framework
UML	Unified Modelling Language