



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
SPORT, ARTS AND CULTURE

APPROVAL PAGE:

**LIMPOPO DEPARTMENT OF SPORT ARTS AND CULTURE
GOVERNANCE OF ICT FRAMEWORK (GICTF), CHARTER
AND IMPROVEMENT ROADMAP**

APPROVAL

**Ms Basani Baloyi
Head of Department**

Date : 13-02-2014



Governance of ICT Framework (GICTF), Charter and Improvement Roadmap for the Limpopo Provincial Administration (LPA)

Document No: **LPPA-00170**

Revision: 1.0

Author: JC Liebenberg

Effective Date: 15 November 2013

Electronic File: LPPA170_1-0



CONFIDENTIAL

Notice

© 2013 SITA. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without the express written permission of SITA.


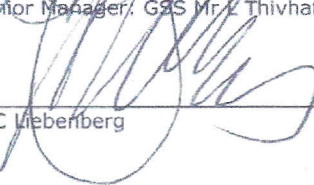
Document enquiries can be directed to:

The Polokwane Configuration Management Office
SITA (Pty) Ltd
PO Box 4777
POLOKWANE
0700

Attention: Mr L Thivhafuni
Telephone: 015 291 8010

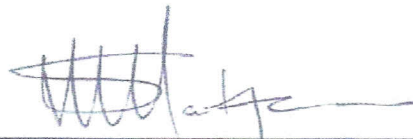
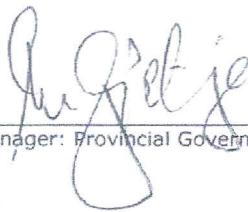

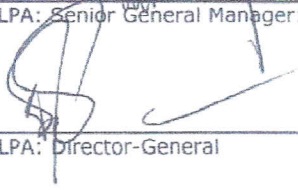
Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

 _____	2013-11-29 Date
Acting Senior Manager: GSS Mr L Thivhafuni	
 _____	2013-11-29 Date
Author: JC Lieberberg	

Client approval

I, the undersigned, hereby accept and approve this SITA LPA Governance of ICT Framework (GICTF), Charter and Improvement Roadmap.

 _____	03/12/13 Date
LPA: Senior Manager: Information and Communication Technology	
 _____	2013.11.29 Date
LPA: General Manager: Provincial Government Information Technology Office	
 _____	09/12/13 Date
LPA: Senior General Manager: Institutional Support Services	
 _____	06/12/2013 Date
LPA: Director-General	

Foreword

This document depicts the IT governance capability maturity status for the LPA, as derived from the IT governance capability maturity assessments conducted. This report also documents the recommended IT Governance Framework and the implementation roadmap for the LPA.

References

1. COBIT Control Practices, Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition, 2007
2. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
3. COBIT 5: Enabling Processes
4. ISACA® Glossary of Terms
5. ICT Governance Capability Assessments, Implementation Roadmaps and ICT Governance Frameworks for the Limpopo Provincial Administration, document LPPA-00138, dated 11 December 2012
6. Office of the Premier, Bid Specification for the Conducting of an Information Technology Governance Maturity Assessment Audit in the Limpopo Provincial Administration and the Development and Formulation of a Provincial Administration-Wide Integrated Information and Communication Technology Governance Framework and Departmental ICT Governance Maturity Improvement Roadmaps, dated June 2011
7. Request for quotation and ICT governance maturity assessment, Governance framework and improvement Framework dated November 2011

Revision

Document number	Revision	Date	Change request	Change comment
LPPA-00170	1.0	29 November 2013	Eventum 1789	New document

Copyright and Trademark

COBIT© 2007 is copyrighted material from the IT Governance Institute™ (ITGI). All rights reserved. www.itgi.org. COBIT® 5 is copyrighted material from © 2012 ISACA®.

CONTENTS

1	Introduction	6
2	Background	6
3	IT Governance Capability Maturity Assessment objectives	7
4	Purpose of this document	7
5	Assessment Approach	7
6	Project Scope	9
6.1	Inclusions	9
6.2	Exclusions	9
7	IT Governance Drivers	9
8.1	Assessment Results (in terms of Performance and Importance)	10
8.1.1	Assessment Results per IT Domain.....	10
8.1.2	Selected IT Processes for the LPA	11
8.2	Summary of findings	11
9	ICT Governance Framework	12
9.1	Purpose of the ICT Governance Framework	12
9.2	ICT Governance Framework Contents.....	12
9.2.1	ICT Governance Principles and Practices	12
9.2.2	ICT Governance Framework	12
9.2.3	Governance Structures	14
9.2.3.1	ICT Strategic Committee.....	15
9.2.3.2	ICT Steering Committee	16
9.2.3.3	ICT Operational Committee	17
9.2.3.4	Audit and Risk Committee.....	17
9.2.4	Corporate Governance of ICT Policy Framework	17
9.2.4.1	Corporate Governance of ICT and Governance of ICT in Perspective.....	17
9.2.4.2	Corporate Governance of ICT Policy Framework Compulsory Programs	18
9.2.4.3	Frameworks	20
9.2.4.4	Processes.....	21
9.2.4.5	Plans	22
9.2.4.6	Policies and Procedures.....	23
9.2.4.6.1	Policies.....	23
9.2.4.6.2	Procedures.....	24
9.2.4.6.3	Governance and Management of Enterprise IT Principles.....	25
9.2.4.6.3.1	Principle 1: Meeting Stakeholder Needs	25
9.2.4.6.3.2	Principle 2: Covering the Enterprise End-to-end.....	25
9.2.4.6.3.3	Principle 3: Applying a Single, Integrated Framework	25
9.2.4.6.3.4	Principle 4: Enabling a Holistic Approach.....	27
9.2.4.6.3.5	Principle 5: Separating Governance from Management	27
9.2.4.6.4	COBIT 5 Enablers.....	28
10	IT Governance Drivers.....	29
11	Information and Communication Technology Corporate Governance of ICT and Governance of ICT RACI Chart	30
12	IT Governance Improvement Roadmap.....	46
12.1	Initiative planning	46
13	Conclusion and way forward	49
13.1	IT Governance COBIT 4.1 Improvement initiatives	49
13.2	CGICTPF Compulsory Programs	49

CONTENTS

Annex A: Definitions	50
Annex B: Overview of COBIT 4.1 Domains and IT Processes.....	52
Annex C: ICT Governance Principles, Practices and Objectives	54
Annex D: LPA ICT Framework-, Processes-, Plans-, Procedures- and Policies Framework	57
Annex E: Rating Scales	71
Annex F: Change Management Methodology.....	72
Annex G: Acronyms.....	73
Annex H: Distribution.....	74

FIGURES

Figure 1: IT Governance Capability Maturity Assessment Framework.....	8
Figure 2: COBIT 4.1 Framework	9
Figure 3: LPA Assessment Results per IT Domain.....	10
Figure 4: Governance Structures for the LPA.....	14
Figure 5: Interrelation of these different Frameworks and Standards.....	18
Figure 6: COBIT 5 Enablers.....	29

TABLES

Table 1: Phases and associated goals.....	8
Table 2: IT Governance Drivers	9
Table 3: LPA Assessment Results per IT Domain.....	10
Table 4: LPA ICT Governance Framework based on COBIT 4.1	12
Table 5: LPA ICT Governance Framework based on COBIT 4.1 mapped to COBIT 5.....	13
Table 6: ICT Strategic Committee Responsibilities.....	15
Table 7: ICT Steering Committee Responsibilities	16
Table 8: ICT Operational Committee Responsibilities.....	17
Table 9: Audit and Risk Committee	17
Table 10: Corporate Governance of ICT Policy Framework	19
Table 11: Required IT Processes.....	21
Table 12: Required ICT Plans	22
Table 13: Required IT Policies	23
Table 14: Required IT Procedures	24
Table 15: COBIT 5 Related Standards	25
Table 16: Related Standards in support of the CGICTPF.....	26
Table 17: CGICTPF and CICTF RACI	30
Table 18: Initiative Planning.....	46
Table 19: Brief overview of the COBIT® domains	52
Table 20: Brief overview of the COBIT® IT processes	52
Table 21: ICT Practices.....	54
Table 22: ICT Frameworks, Processes, Plans, Procedures and Policies Frameworks	57
Table 23: Standards, Legislation, Best practises per IT domain.....	69
Table 24: Performance assessment levels	71
Table 25: Importance Assessment Levels	71
Table 26: Distribution table.....	74

1 Introduction

According to the ISACA® Glossary of Terms, corporate governance is defined as: "The system by which enterprises are directed and controlled. The board of directors is responsible for the governance of their enterprise. It consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives."

Furthermore IT governance is defined as: "The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives."

In the context of the LPA, "the board" as mentioned above, refers to the Executive Council.

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.¹

The LPA acknowledges the importance and advantages of ICT governance and has therefore embarked on an initiative to improve its ICT governance capability maturity levels.

2 Background

According to the LPA Bid Specification, "The Limpopo provincial departments have had matters of emphasis expressed in audit opinions during the last two financial years ending in March 2011. The Limpopo Provincial Government Information Technology Officers Council adopted as far back as August 2006 COBIT, ITIL and ISO 27001 (Code of Practice for Information Security Management) as provincial ICT governance standards, but the implementation of these international standards by provincial department have, at best, been erratic. The Auditor-General has been using for the last two financial years COBIT to assess the status of IT governance in departments, and the departments have been found woefully wanting. Some departments have subsequently attempted to implement ITIL to the total exclusion and neglect of the other standards that also have a bearing on ICT governance. There is thus a need to have a single manual that facilitates the integrated application of all of the international and national standards and that is custom-crafted to the requirements of the Limpopo Provincial Administration."

Based on these requirements SITA conducted IT governance capability maturity assessments, based on COBIT 4.1, for the following departments:

- a. Department of Cooperative Governance, Human Settlements & Traditional Affairs
- b. Department of Agriculture,
- c. Department of Education,
- d. Department of Health,
- e. Department of Public Works,
- f. Department of Safety,
- g. Department of Safety, Security and Liaison,
- h. Department of Social Development,
- i. Department of Sports, Arts and Culture,
- j. The Provincial Treasury,
- k. Department of Economic Development, Environment & Tourism,
- l. Department of Roads and Transport (in 2011) and
- m. The Office of the Premier.

¹ COBIT 5: A Business Framework for the Governance and Management of Enterprise IT

This document must be read in conjunction with the CGICTPF, as adapted by the LPA.

3 IT Governance Capability Maturity Assessment objectives

The assessments were aimed at:

- a) creating awareness on the importance of having an explicit ICT process model in place,
- b) creating ICT governance awareness,
- c) providing insight into COBIT® by focusing on the framework and its respective processes, control objectives and maturity levels,
- d) determining the current and target IT process maturity levels, and
- e) identifying a list of IT Governance improvement initiatives sequenced in priority order.

4 Purpose of this document

This document represents the ICT Governance Capability Maturity Assessment, IT Governance Framework and Charter and Improvement Roadmap for the LPA as a whole, and was derived from the departmental assessments done previously.

5 Assessment Approach

The approach followed the SITA IT Governance Framework, which is based on COBIT 4.1. (See figure below).

Current and required IT governance capability maturity level ratings were requested from departmental IT representatives during conducting of work sessions.

The individual departments were given an opportunity to rate test statements in terms of Performance (To-Be) and Importance (As-Is) related to the COBIT control objectives per IT process. For the rating scales used in assessments in terms of Performance and Importance refer Annex E: Rating Scales

Furthermore the departmental IT representatives had to provide IT-process-related information (Process Attributes) such as who is accountable and responsible and whether or not the process was audited and which software tools are being used to support execution of IT processes.

The Maturity Attributes were not taken into account in defining the recommended improvement initiatives as they are more subjective than the Performance and Importance ratings.

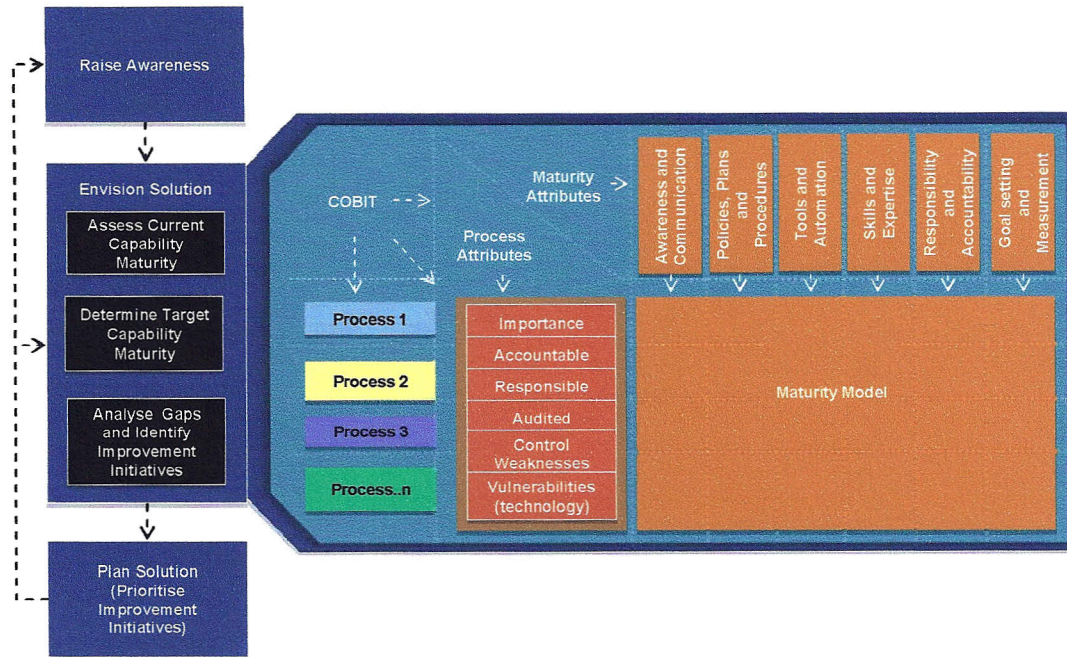


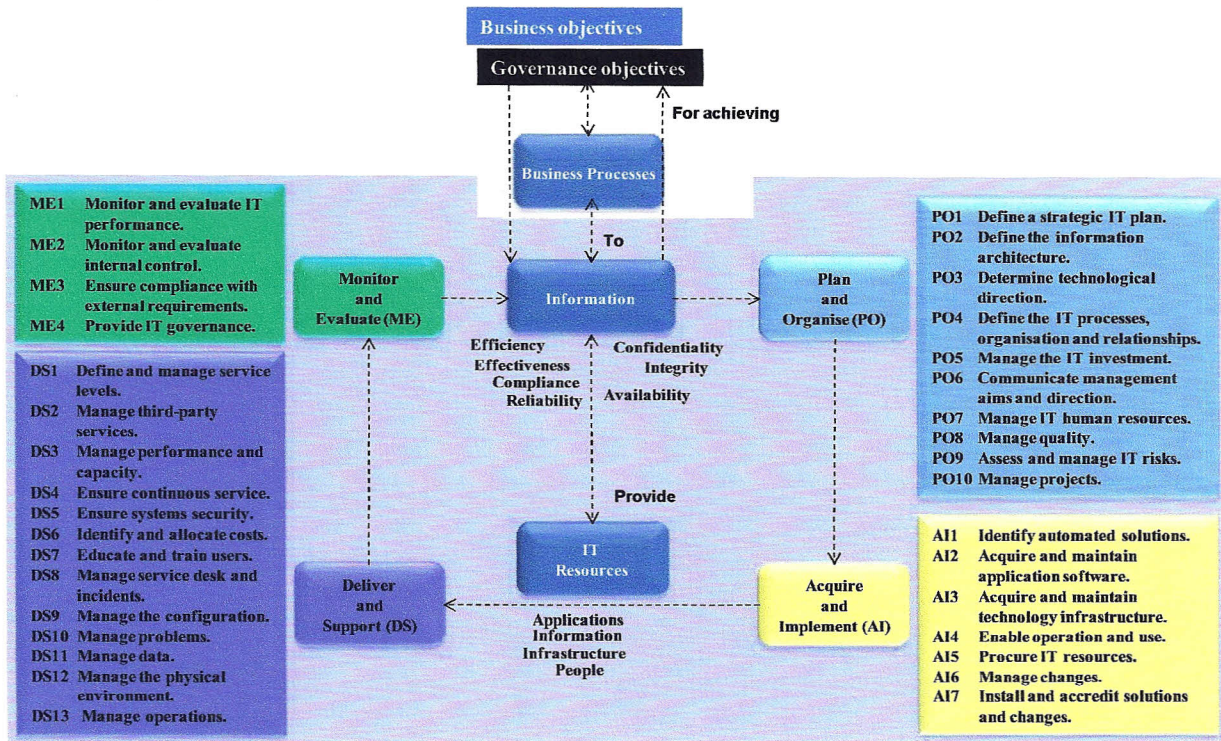
Figure 1: IT Governance Capability Maturity Assessment Framework

The following table lists the goals associated with each phase.

Table 1: Phases and associated goals

Phase	Goal
1. Raise Awareness	To create awareness and importance around IT Governance.
2. Envisage Solution	
Assess Current Capability Maturity	To determine the current IT governance capability maturity level.
Determine target Capability Maturity	To determine the target IT governance capability maturity level.
Analyse Gaps and Identify Improvement Initiatives	To determine the gaps between performance and importance and / or current and target maturity attributes ratings in order to identify improvement initiatives.
3. Plan Solution	To prioritise initiatives.

The assessments covered all 34 COBIT 4.1 IT processes as depicted in the figure below:



Source: Overview of IT Governance and the COBIT Framework, IT Governance Institute

Figure 2: COBIT 4.1 Framework

For a description of the COBIT domains and IT Processes refer Annex B: Overview of COBIT 4.1 Domains and IT Processes.

6 Project Scope

6.1 Inclusions

- The audit reports for departments were studied, analysed and incorporated into the respective departmental reports, and
- Facilitation of the ICT governance capability assessment, and development of ICT Governance framework & improvement roadmap for the LPA using the SITA ICT governance capability maturity assessment framework.

6.2 Exclusions

- assessment of the additional COBIT 5 processes which extend beyond COBIT 4.1,
- detailed analysis of existing IT policies, procedures and processes,
- development of IT related policies, procedures, processes or standards,
- procurement of hardware and software,
- analysis of Government legislation and regulations,
- analysis of business policies, procedures and processes, and
- provision or procurement of any information systems through this project.

7 IT Governance Drivers

The LPA needs to take note of all drivers that impact on IT Governance in terms of acts, regulations, frameworks, standards and reports as depicted below.

Table 2: IT Governance Drivers

Category	Description
Acts and regulations	a) Public Service Act, 1994 b) Preferential Procurement Policy Framework Act No 5 of. 2000,

Category	Description
	c) The Electronic Communications and Transactions Act (Act. No. 25 of 2002), d) Public Service Regulations 2001, as amended 28 April 2006, <ul style="list-style-type: none"> • Chapter 1, Part III:B,C –Strategic Planning, • Chapter 1, Part III.E –Information Planning, • Chapter 5 on e-Government Compliance, e) SITA Act, 88 of 1998 as amended f) SITA General Regulations, 2005 g) Treasury Regulations h) Public Finance Management Act 1 of 1999
Frameworks	a) MTEF, b) Corporate Governance of ICT Policy Framework (CGICTPF), c) CGICTPF Implementation Guide d) Government-wide Enterprise Architecture (GWEA) Framework, and e) Government-Wide Enterprise Architecture (GWEA) Framework Implementation Guide.
Standards	a) National Standards, b) Minimum Interoperability Standards (MIOS), and c) Minimum Information Security Standards (MISS).
Reports	a) Presidential Review Commission Report, 1998, Chapter 5 b) King III report on Corporate Governance for South Africa, 2009, Chapter 5: The governance of information technology.
Directives	(a) National Treasury Practice Notes

8.1 Assessment Results (in terms of Performance and Importance)

8.1.1 Assessment Results per IT Domain

The figure below depicts the assessment results for the four IT domains in graphic detail.

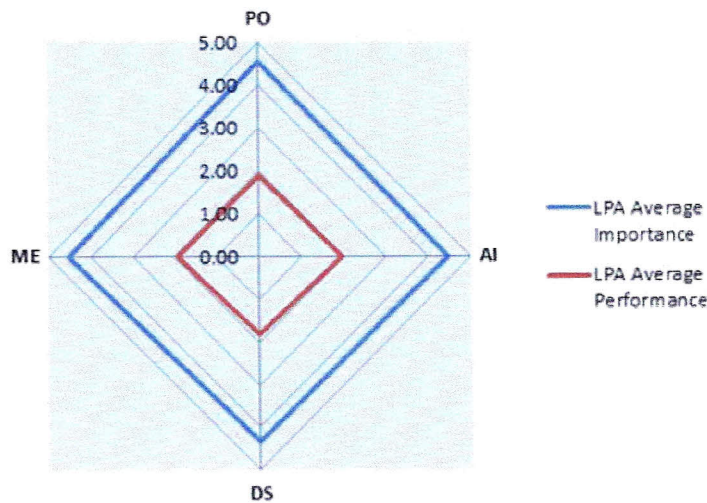


Figure 3: LPA Assessment Results per IT Domain

The table below shows that in terms of Importance the ME domain was rated highest. However in terms of performance it was also rated highest together with the AI domain. As such no initiatives were derived for it. The DS domain was rated the lowest in terms of Performance.

Table 3: LPA Assessment Results per IT Domain

Description	PO	AI	DS	ME	Average
LPA Average Importance	4.52	4.45	4.32	4.53	4.45
LPA Average Performance	1.86	1.96	1.81	1.96	1.90
% Difference	143.0%	127.0%	138.7%	131.1%	134.2%

For a description of the rating scales refer: Annex E: Rating Scales.

8.1.2 Selected IT Processes for the LPA

Based on the assessments for the LPA departments, a list of recommended IT processes to be implemented was selected as follows:

- a) The top 10 processes, based on greatest gap between Performance and Importance per department were selected,
- b) These selected IT processes were averaged and prioritised
- c) The top fifteen (15), based on greatest gap between Performance and Importance, were selected.
- d) DS13 Manage Operations and AI4 Enable Operation and Use were deleted from the list, as they were deemed not important enough in the context of the exercise.

The list of selected IT processes is depicted below. A mapping to the relevant COBIT 5 process reference is also shown:

IT Process	COBIT 5 Process Reference	% Difference
a) PO2 Define the Information Architecture	a. APO01 b. APO03	300
b) PO3 Determine Technological Direction	a. APO01 b. APO02 c. APO03 d. APO04	313
c) PO4 Define the IT Processes, Organisation and Relationships	a. APO01 b. APO07 c. APO11	301
d) PO8 Manage Quality	a. APO11	280
e) PO9 Assess and Manage IT Risks	a. EDM03 b. APO01 c. APO12	374
f) PO10 Manage Projects	a. BAI01	268
g) AI2 Acquire and Maintain Application Software	a. BAI03	273
h) AI6 Manage Changes	a. BAI06	269
i) AI7 Install and Accredite Solutions and Changes	a. BAI05 b. BAI07	264
j) DS4 Ensure Continuous Service	a. DSS04	279
k) DS10 Manage Problems	a. DSS03	296
l) DS8 Manage Service Desk and Incidents	a. DSS02	258
m) DS9 Manage the Configuration	a. BAI10 b. DSS02	294

Source: Mapping table: COBIT 5©, Enabling Processes, an ISACA® Framework.

The ICT Process Framework is based on these initiatives per ICT process. As the % difference for all these initiatives are >= 150%, they are all classified as a priority one: translating to "needs urgent attention".

8.2 Summary of findings

The average rating for the organisation is at 1.90 which is below 2.

According to the COBIT Generic Model, the general description for a level 1 is: 'Initial/Ad Hoc - There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.'

The description for a level 2 is: "Repeatable but Intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left

to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

Other findings are:

- a) There is no explicit ICT process framework in place,
- b) There are limited formal ICT policies, processes, procedures or plans instituted,
- c) A number of ICT processes have not been audited,
- d) There are limited tools used in support of executing the ICT processes. Desktop productivity tools are primarily used and have limited functionality to support effective and efficient execution of the ICT processes and
- e) ICT strategic plans are either in process of being finalized or are non-existent.

9 ICT Governance Framework

9.1 Purpose of the ICT Governance Framework

The purpose of this framework is to outline what the LPA is going to utilise in the execution of its IT governance activities.

This framework will also touch on addressing:

- a) the LPA’s compliance to the King III report in terms of an ICT Governance Framework,
- b) guiding the development of frameworks, policies, structures and procedures,
- c) ensuring compliance with applicable laws and regulations in context, and
- d) assist in resolving ICT Governance related AG findings.

9.2 ICT Governance Framework Contents

9.2.1 ICT Governance Principles and Practices

For the principles, practices and objectives applicable to the LPA, as per the CGICTF, refer to Annex C: ICT Governance Principles, Practices and Objectives.

9.2.2 ICT Governance Framework

In the frameworks that follow, the intent of the four ICT domains should be kept in mind. Refer Annex B: Overview of COBIT 4.1 Domains and IT Processes for a description.

The figure below depicts the ICT Governance Framework which needs to be developed and maintained by the LPA. It includes a framework, policies, processes, plans, procedures, decision and reporting structures for ICT and accountability structures.

Table 4: LPA ICT Governance Framework based on COBIT 4.1

IT Governance Framework for the LPA	Category	Plan and Organize	Acquire and Implement	Deliver and Support	Monitor and Evaluate
	Frameworks	PO4.1, PO9.1 PO10.2, PO10.9	AI6.1	DS4.1	
	Processes	PO3.3, PO3.4, PO3.5, PO4.5, PO4.10, PO8.2, PO9.5, PO10.2	AI2.9, AI2.10, AI6.2, AI6.3, AI6.4, AI7.8,	DS4.7, DS8.3, DS8.4, DS8.5, DS9.1, DS9.2, DS9.3, DS10.1, DS10.3, DS10.4	
	Policies	PO4.9, PO4.14, PO8.3,		DS4.1, DS9.2	
	Plans	PO3.1, PO3.2, PO4.1, PO8.1, PO8.5, PO9.5,	AI2.1, AI2.2, AI2.8, AI2.10, AI6.4, AI7.1,	DS4.2	

CONFIDENTIAL

I T G	Category	Plan and Organize	Acquire and Implement	Deliver and Support	Monitor and Evaluate
		P010.5, PO10.7, PO10.10	AI7.2, AI7.3, AI7.9,		
	Procedures	PO2.4, PO4.9, PO4.12, PO4.13, PO8.2, PO8.3,	AI2.7, AI6.1, AI7.2, AI7.8, AI7.9,	DS4.1, DS4.2, DS4.4, DS4.7, DS4.8, DS4.10, DS8.1, DS8.3, DS8.4, DS9.2, DS10.2, DS10.3	
	Decision Reporting and structures for IT decisions	PO3.5, PO4.2, PO4.3			ME4.1
	Accountability Structures	Provincial Government Information Technology Office (Head of Department)	Head of Department	Head of Department	Head of Department
Responsibility Structures	LPA Departments	LPA Departments	LPA Departments	LPA Departments	

Refer Annex D: LPA ICT Framework-, Processes-, Plans-, Procedures- and Policies Framework for a full depiction of the target LPA environment.

Table 5: LPA ICT Governance Framework based on COBIT 4.1 mapped to COBIT 5

IT Governance Framework for the LPA	Category	Align, Plan and Organize (APO)	Build, Acquire and Implement (BAI)	Deliver, Service and Support (DSS)	Monitor, Evaluate and Assess (MEA)
	Frameworks	APO01.03, APO01.07, EDM03.02, BAI01.01, BAI01.10	BAI06.01, BAI06.02, BAI06.03, BAI06.04	DSS04.01, DSS04.02	
	Processes	EDM01.01, APO04.03, APO03.05, APO01.01, APO11.02, APO12.06, BAI01.01	BAI03.09, BAI03.10, BAI06.01, BAI06.02, BAI06.03, BAI07.06	DSS04.03, DSS02.04, DSS02.05, DSS02.06, DSS02.07 BAI10.01, BAI10.02, BAI10.04, DSS02.01, BAI10.03, BAI10.04, BAI10.05, DSS02.05, DSS03.01, DSS03.03, DSS03.04, DSS03.05	
	Policies	APO01.06, APO07.06, APO11.02, APO11.05		DSS04.01 DSS04.02, BAI10.03	
	Plans	APO02.03, APO04.03, APO02.03,	BAI03.01, BAI03.02, BAI03.06,	DSS04.03	

IT Governance	Category	Align, Plan and Organize (APO)	Build, Acquire and Implement (BAI)	Deliver, Service and Support (DSS)	Monitor, Evaluate and Assess (MEA)
		APO02.04, APO02.05, APO04.03, APO04.04, APO04.05, APO01.03, APO01.07, APO11.01, APO11.06, APO12.06, BAI01.07, BAI01.08, BAI01.09	BAI03.10, BAI06.03, BAI05.05, BAI07.01, BAI07.03, BAI07.01, BAI07.08		
	Procedures	APO01.06, APO07.01, APO07.02, APO11.02, APO11.05	BAI03.03, BAI03.04, BAI06.01, BAI06.02, BAI06.03, BAI06.04, BAI07.01, BAI07.03, BAI07.06, BAI07.08	DSS04.01, DSS04.02, DSS04.03, DSS04.04, DSS04.06, DSS04.09, DSS02.04, DSS02.05, DSS02.06, BAI10.03, DSS03.02, DSS03.03, DSS03.04	
	Decision Reporting and structures for IT decisions	APO01.01			EDM01.01
	Accountability Structures	Provincial Government Information Technology Office (Head of Department)	Head of Department	Head of Department	Head of Department
Responsibility Structures	LPA Departments	LPA Departments	LPA Departments	LPA Departments	

Note that Control Objective DS8.1 (Service Desk) has been deleted in COBIT 5 as ITIL 3 does not refer to Service Desk as a process.

9.2.3 Governance Structures

The figure below illustrates the dynamics between the different governance structures.

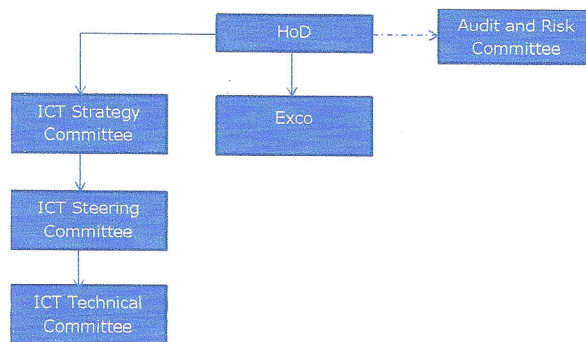


Figure 4: Governance Structures for the LPA

It is important to note that the HOD needs to provide strategic leadership, whilst the Exco needs to provide the political leadership.

9.2.3.1 ICT Strategic Committee

This committee operates on an executive level as depicted in the table below. The ICT Strategic Committee conceptualises and oversees the CGICT, GICT and strategic alignment.

The table below depicts the responsibilities, chairperson and members of the committee.

Table 6: ICT Strategic Committee Responsibilities

Responsibilities			Chairperson / Members
Evaluate	Conceptualise and direct	Monitor	
<p>Evaluate the departmental strategic plan, internal and external environment to:</p>	<p>Conceptualise and direct business enablement by ICT arrangements:</p>	<p>Monitor that implementation conforms to the criteria:</p>	<p>Provincial Administration (PSA Schedule 1) Level:</p> <p>Chair: Director-General Members: Heads of department, Designated Provincial Governance Champion (GC), Designated Provincial Enterprise Architect and Provincial GITO.</p> <p>Department (PSA Schedule 2) Level:</p> <p>Chair: Head of department Members: Members of Executive Management Committee, Designated Governance Champion, Designated Enterprise Architect, and GITO</p>
<p>a) Identify stakeholder needs and how it should be realised b) Determine value ICT is expected to create through its enablement of the business c) Define the benefits ICT is expected to realise in its enablement of business d) Articulating ICT risk appetite and how it should be management within the risk management regime of the department e) Facilitate the establishment of sufficient ICT organisational structure, resources, capacity and capability f) Evaluate and</p>	<p>a) Ensure integration of CGICT into the agenda of the Executive Committee b) Approve CGICT Policy and Charter c) ICT Plan, ICT Implementation Plan (MTEF) d) ICT Operational Plan (APP) and other related plans and policies e) Approve portfolio of ICT projects and its related expenditure f) Provide direction for the change management requirements for the implementation of CGICT g) Guide implementation of the Framework and related policies and strategies</p>	<p>a) Conformance, performance and assurance oversight and monitoring b) Ensure that risk is managed and the ICT is audited internally and independently</p>	

Responsibilities			Chairperson / Members
Evaluate	Conceptualise and direct	Monitor	
monitor significant ICT expenditure g) Determine the monitoring criteria and reporting requirements h) Broadly understand the implications of the ICT prescriptive environment i) Evaluate the change management requirements for the implementation of CGICT			

9.2.3.2 ICT Steering Committee

This committee also operates on an executive level. This committee coordinates and oversees the planning, implementation and execution of the CGICT, GICT and strategic alignment and related monitoring activities.

The table below depicts the responsibilities, chairperson and members of the committee.

Table 7: ICT Steering Committee Responsibilities

Responsibilities			Chairperson / Members
Evaluate:	Direct:	Monitor:	
a) Coordinate development of CGICT Policy b) Coordinate planning based on direction received from the ICT Strategic Committee c) Determine, prioritise and recommend plans, policies, strategies, resource/capacity requirements, portfolios of ICT projects and risk management to ICT Strategic Committee and/or HoD d) Oversee the identification of the ICT prescriptive environment	a) Oversee the implementation of approved plans, policies, strategies, resource/capacity requirements, risk management, benefits realisation, portfolios of ICT projects, internal and external audits b) Determine the monitoring criteria and related reporting requirements and processes for conformance, performance and assurance c) Provide direction to all ICT related decisions that may have an impact on the business operations and culture of the department that is escalated to the Committee d) Determine the change management requirements for the implementation of CGICT and report to Strategic Committee	a) Conformance, performance and assurance monitoring and reporting to ICT Strategic Committee b) Oversee and report on the change management implementation for the implementation of CGICT	Provincial Administration (PSA Schedule 1) Level: Chair: Provincial GITO Members: Departmental GITOs, Designated Provincial Governance Champion, Designated Provincial Enterprise Architect, SITA Provincial Manager. Provincial Internal Audit representative, Head of Financial Information Systems in the Provincial Treasury Department (PSA Schedule 2) Level: Chair: Member of the Executive Management Committee designated as such by the Accounting Officer of the department Members: Other designated members of the Executive Management Committee representing line functions, Designated Governance Champion, Designated Enterprise Architect, GITO and Head of Risk Management

9.2.3.3 ICT Operational Committee

This committee operates on an operational level. This committee keeps track of the day-to-day ICT service management elements and reporting requirements.

The table below depicts the responsibilities, chairperson and members of the committee.

Table 8: ICT Operational Committee Responsibilities

Responsibilities	Chairperson / Members
a) Provide input into the development of the ICT Plan, ICT Implementation Plan and ICT Operational Plan b) Govern and Manage the ICT Framework and ICT Project Program c) Coordinate implementation of ICT Plan, ICT Implementation Plan, ICT Operational Plan and ICT Project Program d) Day-to-day operational and service management e) Manage ICT risks f) Conformance and performance reporting to ICT Steering Committee	Chairperson: GITO Members: Business line functionaries and ICT management functionaries.

9.2.3.4 Audit and Risk Committee

This committee reports on the adequacy of controls in the LPA.

The table below depicts the responsibilities, chairperson and members of the committee.

Table 9: Audit and Risk Committee

Responsibilities	Chairperson / Members
a) The group of executives of the enterprise who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee b) ensure that IT risks are adequately addressed c) obtain appropriate assurance that controls are in place and effective in addressing IT risks d) should consider IT as it relates to financial reporting and the going concern of the company e) consider the use of technology to improve audit coverage and efficiency	Chairperson: Audit / Risk Committee member Members: Business and ICT representatives

9.2.4 Corporate Governance of ICT Policy Framework

9.2.4.1 Corporate Governance of ICT and Governance of ICT in Perspective

The figure below depicts the various layers of governance and the interrelationship between these different Frameworks and Standards.

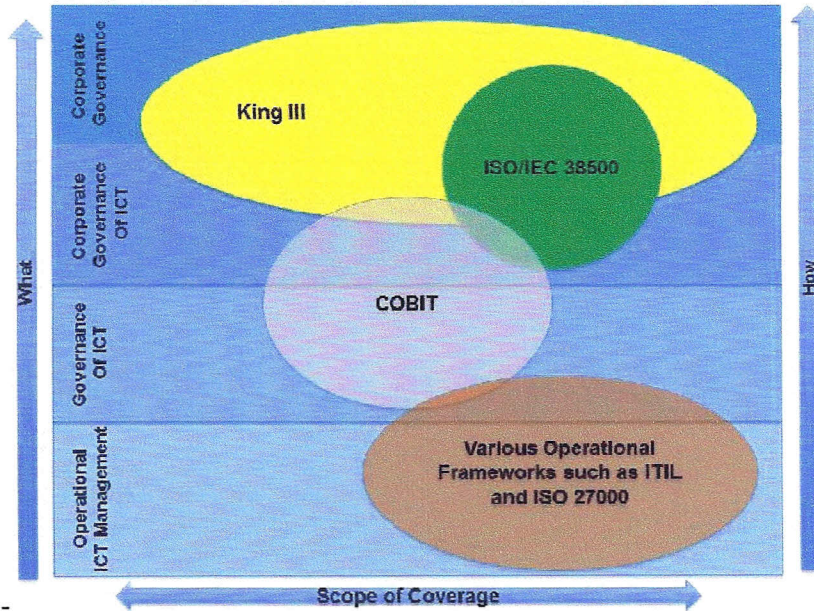


Figure 5: Interrelation of these different Frameworks and Standards

In the context of the South African Government, according to the DPSA’s Public Service Corporate Governance of Information and Communication Technology Framework (CGICTF), the purpose of ICT is to serve as an enabler of public service delivery through, inter alia, achieving the ICT House of Values and key focus areas to enable the Public Service to achieve the 12 strategic outcomes.

Furthermore the importance of ICT Governance has been highlighted by the King III Report and Code on Governance for South Africa (chapter 5: The Governance of Information Technology), the Presidential Review Commission report of 1998 and audit findings by the Auditor General (AG).

Legend:

- ISO/IEC 38500:2008. Corporate governance of information technology.
- ISO/IEC 27000:2009. Information security management systems.

9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs

The CGICTPF requires departments to implement the corporate governance of ICT (CGICT) and Governance of ICT (GICT) as an integral part of their corporate governance arrangements. A phased implementation approach is followed that should be completed by the dates indicated.

There are three compulsory phases, with phase one deliverables due by March 2014, phase two deliverables due by March 2015 and Phase 3 from April 2015 onwards concentrating on continuous improvement of governance and strategic alignment between ICT and government business.

The table below depicts the deliverables to be produced according to the *Implementation Guideline for Corporate Governance of Information and Communication Technology Policy Framework I (CGICTPF), version 1*, with mappings to the relevant COBIT 5 processes. Also included is a depicting of the COBIT 5, seven enablers mapped to the relevant IT process reference.

Table 10: Corporate Governance of ICT Policy Framework

Category	Deliverable / Enabler	EDM	APO							BAI	DSS			MEA	CGICTPF	
		EDM01	APO01	APO02	APO03	APO05	APO10	APO12	APO13	BAI01	DSS01	DSS04	DSS05	MEA01		
Capabilities	Designation of a Governance Champion to coordinate the development and implementation of the CGICT															X
Frameworks	ICT Portfolio Management Framework					X										
	Governance and Management of ICT Framework	X	X	X				X	X	X	X	X		X	X	
Policies	LPA CGICT Policy	X	X	X							X			X	X	
	a) Risk Management Policy with relation to ICT							X							X	
	b) ICT Security Policy				X				X				X		X	
Charter	LPA CGICT Policy Charter	X	X	X							X			X	X	
Plans	a) Internal Audit plan that includes ICT															X
	b) Business Continuity Plan (BCP)				X					X		X	X			X
	c) ICT Continuity Policy and Plan				X					X		X	X			X
	d) Change management Plan for the implementation of CGICT and GICT															X
	e) Enterprise Architecture (including an Information plan and ICT Business Engagement Plan.)		X		X	X	X	X	X	X	X			X	X	
COBIT 5 Enablers	Principles, policies and frameworks	X	X													
	Processes	X	X													
	Organisational structures	X	X													
	Culture, ethics and behaviour	X	X													
	Information				X											
	Services, infrastructure and applications				X											
People, skills and competencies (not part of the CGICTPF):																

IT	Category	Deliverable / Enabler	EDM	APO							BAI	DSS			MEA	CGICTPF
			EDM01	APO01	APO02	APO03	APO05	APO10	APO12	APO13	BAI01	DSS01	DSS04	DSS05	MEA01	
		APO07														

The ICT plans, ICT implementation plans and ICT operational plans have been replaced with Enterprise Architecture, based on GWEA.

Note that besides the COBIT 5 processes indicated above, there are more drivers that need to be taken into consideration during development of these deliverables e.g. Public Service Regulations (PSR), National Treasury (NT) Strategic Planning Framework (FW), Annual Performance Plan (APP), Estimates of National Expenditure (ENE), Medium Term Expenditure Framework (MTEF), Government Wide Enterprise Architecture (GWEA), Minimum Interoperability Standards (MIOS), Minimum Information Security Standards (MISS), etc.

The implementation of the Framework will be monitored for conformance by the Department Public Service and Administration (DPSA), performance by the Department of Planning, Monitoring and Evaluation (DPME) and audited by the AG.

Conformance to the Framework will be monitored on an annual basis through the utilisation of the Corporate Governance of Information and Communication Technology Assessment Standard which is aligned with that of the Management Performance Assessment Tool (MPAT).

9.2.4.3 Frameworks

The LPA will be operating the following frameworks. These frameworks are as a result of the IT Capability Maturity assessment that was done and they include the following:

- a) **Government Wide Enterprise Architecture Framework (GWEA)**, which is a norm for developing ICT plans for government;
- b) **ICT Process Framework**, which is a supporting framework required to enable the definition and follow-up of process goals, measures, control and maturity;
- c) **ICT Risk and Control Framework** to document a common and agreed-upon level of IT risks, mitigation strategies and residual risks.
- d) **Portfolio, Programme and Project Management Framework** which defines the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. The LPA has considered adopting the United Kingdom Office of the Government Commerce Portfolio, Programme and Project Management Maturity Model (P3M3) methodology, which supplies standard terminology and guidelines for project management and which includes the PProjects IN Controlled Environments (PRINCE2), which is a de facto process-based method for effective project management.
- e) A **change management framework** that specifies the policies and processes, including:
 - i. Roles and responsibilities
 - ii. Classification and prioritisation of all changes based on business risk
 - iii. Assessment of impact
 - iv. Authorisation and approval of all changes by the business process owners and IT
 - v. Tracking and status of changes
 - vi. Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention)
 - vii. The SITA Change Management Framework will be the standard that is adopted for change management.
- f) **ICT Service Continuity Framework**, to support business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans.

9.2.4.4 Processes

The LPA ICT Governance Framework includes a process framework, and it includes processes as indicated as part of Annex D: LPA ICT Framework-, Processes-, Plans-, Procedures- and Policies Framework. The process framework is grouped according to the COBIT domains i.e. Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (ME).

Table 11: Required IT Processes

Domain (COBIT 4.1 / COBIT 5)	ICT Processes		
	Control Objective	COBIT 5 Process Reference	IT Process Description
PO / APO	PO3.3	EDM01.01; APO04.03	Establish a process to monitor the business sector, industry, technology, infrastructure, legal and regulatory environment trends. Incorporate the consequences of these trends into the development of the IT technology infrastructure plan
	PO3.4	APO03.05	Establish a process to prevent the acquisition of non-conforming systems or applications. A monitoring and benchmarking process, such as measuring non-compliance to technology standards, to ensure compliance to the standards.
	PO3.5	APO01.01	A process in place to monitor and benchmark the effect on business strategy and identify instances of non-compliance to technology standards.
	PO4.8	Deleted - these specific roles are no longer explicitly specified as a practice.	NA
	PO4.10	APO01.02	A process for escalating issues that are identified through supervisory processes.
	PO9.5	APO12.06	A risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels
	PO10.2	BAI01.01	A change control process for recording, evaluating, communicating and authorising changes to the project scope, project requirements or system design
AI / BAI	AI2.9	BAI03.09	A process for standardising, tracking, recording and approving all change requests during development of application systems.
	AI2.10	BAI03.10	A process for application software maintenance activities.
	AI6.2	BAI06.01	A process to allow business process owners and IT to request changes to infrastructure, systems or applications.
	AI6.3	BAI06.02	A process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process
	AI6.3	BAI06.02	Processes within the overall change management process to declare, assess, authorise and record an emergency change.
	AI6.4	BAI06.03	A process to allow requestors and stakeholders to track the status of requests throughout the various stages of the change management process.
	AI7.4	BAI07.04	A process to enable proper retention or disposal of test results, media and other associated documentation to enable adequate review and subsequent analysis as required by the test plan.
DS / DSS	DS4.7	DSS04.03	A distribution process that: a) Distributes the IT continuity plan in a timely manner to all recipients and locations on the distribution list b) Collects and destroys obsolete copies of the plan in line with the organisation's policy for discarding confidential information
	DS8.3	DSS02.04	a) A process to ensure that the incident records are updated to show the date, time and assignment to IT personnel. A process to ensure that IT staff members dealing with customer queries update the request or incident records with relevant information, such as classification, diagnosis, root cause and workarounds
	DS8.4	DSS02.05;	A process to manage the resolution and closure of each incident,

Domain (COBIT 4.1 / COBIT 5)	ICT Processes		
	Control Objective	COBIT 5 Process Reference	IT Process Description
		DSS02.06	including use of predetermined categorisations to identify the likely root cause of the incident.
	DS8.5	DSS02.07	A process to identify, investigate and report on all queries in which the agreed-upon time frames for resolution (e.g., SLAs) were exceeded.
	DS9.1	BAI10.01; BAI10.02; BAI10.04; DSS02.01	A process to revert to the baseline configuration in the event of problems, if determined appropriate after initial investigation.
	DS9.2	BAI10.03	a) A process to record new modified and deleted configuration items and their relative attributes and versions. Identify and maintain the relationships between configuration items in the configuration repository. b) A process to maintain an audit trail for all changes to configuration items. Define a process to identify critical configuration items in relationship to business functions (component failure impact analysis). c) A process to ensure that valid licences are in place to prevent the inclusion of unauthorised software
	DS9.3	BAI10.04; BAI10.05; DSS02.05	A process to ensure that configuration items are monitored. Compare recorded data against actual physical existence, and ensure that errors and deviations are reported and corrected.
	DS10.1	DSS03.01	A process to report and classify problems that have been identified as part of incident management.
	DS10.1	DSS03.01	Define and implement a problem-handling process that has access to all relevant data, including information from the change management system and IT configuration/asset and incident details, to effectively address the root cause(s).
	DS10.3	DSS03.03; DSS03.04	A process to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.
	DS10.4	DSS03.05	A process to capture problem information related to IT changes and to communicate it to key stakeholders.

Source: Mapping table: COBIT 5©, Enabling Processes, an ISACA® Framework.

Furthermore, the process framework also indicates the relevant legislative framework for each COBIT domain. The legislative framework shall inform the development of certain ICT processes within the LPA.

9.2.4.5 Plans

The LPA, like any government entity, is expected to develop its own planning cycles within the overall planning framework of Government as agreed by Cabinet. The planning Framework includes a sequence of activities that will culminate each year with a Medium Term Strategic Framework (MTSF) - a limited but focused set of medium-term strategic objectives that are shared by all spheres of government and inform the Medium Term Expenditure Framework (MTEF) that has been in operation for some time.

The LPA has adopted the GWEA and TOGAF as frameworks for developing ICT plans, as GWEA is the norm for developing ICT plans in government.

Furthermore, as a result of the IT governance capability assessment that was done, the LPA also needs to develop plans as indicated below. These plans are grouped according to the process domains as specified in COBIT 4.1.

Table 12: Required ICT Plans

Domain (COBIT 4.1 / COBIT 5)	ICT Plans		
	Control Objective Reference	COBIT 5 Process Reference	Plan Name and/or Description
PO / APO	PO3.1	APO02.03; APO04.03	Technological Direction plan.
	PO3.2	APO02.03;	Technology Infrastructure Plan

Domain (COBIT 4.1 / COBIT 5)	ICT Plans		
	Control Objective Reference	COBIT 5 Process Reference	Plan Name and/or Description
		APO02.04; APO02.05; APO04.03; APO04.04; APO04.05	
	PO4.1	APO01.03; APO01.07	IT process framework
	PO8.1	APO11.01	Project quality plans
	PO8.5	APO11.06	A quality plan that promotes continuous improvement.
	PO9.5	APO12.06	A risk action plan
	PO10.5	BAI01.07	A project communication plan that identifies internal and external project communications.
	PO10.7	BAI01.08	Integrated Project Plans
	PO10.10	BAI01.09	Project Quality Plan
AI / BAI	AI2.8	BAI03.06	Software QA plans
	AI2.10	BAI03.10	A plan for the maintenance of software applications.
	AI7.1	BAI05.05	Training and implementation plan
	AI7.1	BAI05.05	Implementation and fall-back /back out plans
	AI7.9	BAI07.08	Action plan to address issues identified in the post-implementation review.
DS / DSS	DS4.2	DSS04.03	IT Continuity Plans

Source: Mapping table: COBIT 5©, Enabling Processes, an ISACA® Framework.

9.2.4.6 Policies and Procedures

Policies and procedures help new staff familiarise themselves with the service’s practised and gives them information about what to expect from the service. Policies should be ‘living’ documents that must be regularly reviewed to ensure that they meet all the needs of those working in the service, and should take into account the possible changes that have happened in the service and within the wider community.

Well thought-out and implemented policies and procedures:

- a) Ensure adherence to good practices,
- b) help to establish a professional and effective organisation,
- c) provide consistency amongst staff,
- d) prevent any ambiguity about how particular situations/issues should be handled in the service,
- e) promote harmony among staff,
- f) ensure efficient and effective delivery of services, and
- g) provide confidence in decision-making.

9.2.4.6.1 Policies

The services rendered by GITO units in departments need to have policies and procedures to help them guide the actions of all individuals involved in the service. They ensure and endorse the well-being of all staff and everyone who is connected to the service. When policies and procedures are well thought out and, most importantly, implemented, they provide common understanding and agreement on how things should be done at the service level. Procedures provide clear instructions and guidelines on what should/must be done in a particular set of circumstances or with regard to a particular issue.

Table 13: Required IT Policies

Domain (COBIT 4.1 / COBIT 5)	Policies		
	Control Objective Reference	COBIT 5 Process Reference	Name and/or Description
PO / APO	PO4.9	APO01.06	Policies to ensure appropriate and consistent enterprise wide classification of data.
	PO4.14	APO07.06	Contracted staff policies and procedures
	PO8.3	APO11.02; APO11.05	Policies, as part of the development and acquisition standards, that provide appropriate and ‘fit for purpose’ guidelines for controlled

CONFIDENTIAL

Domain (COBIT 4.1 / COBIT 5)	Policies		
	Control Objective Reference	COBIT 5 Process Reference	Name and/or Description
			development
DS / DSS	DS4.1	DSS04.01; DSS04.02	Policies for conducting regular IT Continuity tests
	DS9.2	BAI10.03	A policy that integrates incident, change and problem management procedures with the maintenance of the configuration repository.

Source: Mapping table: COBIT 5©, Enabling Processes, an ISACA® Framework.

9.2.4.6.2 Procedures

The table below indicate the procedures that form part of the LPA's ICT Governance Framework.

Table 14: Required IT Procedures

Domain (COBIT 4.1 / COBIT 5)	Procedures		
	Control Objective Reference	COBIT 5 Process Reference	Name and/or Description
PO / APO	PO2.4	APO01.06	Procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.
	PO2.4	APO01.06	Procedures to manage and maintain data integrity and consistency throughout the complete data process and life cycle
	PO4.9	APO01.06	Data and system ownership procedures
	PO4.12	APO07.01	Procedures to address the maintenance of appropriate segregation of duties and responsibilities during periods when regular personnel are unavailable
	PO4.13	APO07.02	Job procedures for key processes.
	PO8.2	APO11.02	IT quality practices procedures
	PO8.3	APO11.02; APO11.05	Procedures, as part of the development and acquisition standards, that provide appropriate and 'fit for purpose' guidelines for controlled development
AI/ BAI	AI2.7	BAI03.03; BAI03.04	Development procedures
	AI6.1	BAI06.01; BAI06.02; BAI06.03; BAI06.04	Change management procedures for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.
	AI7.8	BAI07.06	A procedure to log what software and configuration items have been distributed, to whom, where they have been implemented, and when each has been updated
	AI7.9	BAI07.08	Post-implementation procedures
	AI7.9	BAI07.08	Procedures for post-implementation reviews
DS / DSS	DS4.1	DSS04.01; DSS04.02	Documentation standards and change management procedures for all IT continuity-related procedures and tests
	DS4.2	DSS04.03	Emergency procedures to ensure the safety of all affected parties, including coverage of occupational health and safety requirements
	DS4.4	DSS04.02; DSS04.06	Change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements.
	DS4.7	DSS04.03	Procedures documenting instructions for storage of confidential information.
	DS4.8	DSS04.04	Resumption procedures.
	DS4.10	DSS04.09	Procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster
	DS8.1	Deleted— ITIL 3 does not refer to Service Desk as a process.	NA
	DS8.3	DSS02.04	Service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided.
	DS8.4	DSS02.05;D SS02.06	Procedures for the monitoring of timely clearance of customer queries.
	DS9.2	BAI10.03	Configuration procedures to support management and logging of all changes to the configuration repository
DS10.2	DSS03.02	Problem management procedures for the tracking of problem trends.	

Domain (COBIT 4.1 / COBIT 5	Procedures		
	Control Objective Reference	COBIT 5 Process Reference	Name and/or Description
	DS10.3	DSS03.03;D SS03.04	A procedure to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.

Source: Mapping table: COBIT 5©, Enabling Processes, an ISACA® Framework.

9.2.4.6.3 Governance and Management of Enterprise IT Principles

COBIT 5 contains 5 principles that aim to enable the LPA to create an effective governance and management framework in order to optimise information and technology investments to the benefit of stakeholders. Also refer Annex C: ICT Governance Principles, Practices and Objectives as has been adopted by the LPA.

These principles are:

9.2.4.6.3.1 Principle 1: Meeting Stakeholder Needs

Government exists to create value for their stakeholders, mainly the citizens of the country, by maintaining a balance between the realisation of benefits and the optimisation of risk and use of resources.

Business goals should be cascaded, and translated into manageable, specific, IT-related goals which should be mapped to specific processes and practices.

9.2.4.6.3.2 Principle 2: Covering the Enterprise End-to-end

As COBIT 5 integrates governance of enterprise IT into enterprise governance:

- a. It covers all functions and processes within the LPA; not only on ICT, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the LPA.
- b. It considers all IT-related governance and management enablers to be LPA wide and end-to-end, i.e., inclusive of everything and everyone—internal and external—that is relevant to governance and management of enterprise information and related IT.

9.2.4.6.3.3 Principle 3: Applying a Single, Integrated Framework

COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT as depicted below:

Table 15: COBIT 5 Related Standards

#	Standard	Description
1.	ITIL V3 2011 (Information Technology Infrastructure Library)	Service Management
2.	COSO/ERM	Enterprise Risk Management
3.	ISO/IEC 20000	IT Service Management
4.	ISO/IEC 27001	Information Security Management Systems
5.	ISO/IEC 27002	Information Security Foundation
6.	ISO/IEC 31000	Risk Management
7.	ISO/IEC 38500	IT Governance Standard
8.	ISO/IEC 9001	Quality management systems
9.	King III	Corporate and IT Governance
10.	NA	Kotter, John; <i>Leading Change</i> , Harvard Business School Press, USA, 1996 (Change Management)
11.	NIST SP800-53 Rev 1 (National Institute of Standards and Technology)	Risk Management Guide for Computer Security
12.	OECD (Organisation for Economic Co-operation and Development)	Corporate Governance Principles
13.	PRINCE2 (projects in controlled	Project Management

CONFIDENTIAL

#	Standard	Description
	environments, version 2)	
14.	PMBOK (Project Management Body of Knowledge)	Project Management
15.	SFIA (Skills Framework for the Information Age)	A model for describing and managing competencies for ICT professionals for the 21st century, and is intended to help match the skills of the workforce to the needs of the business.
16.	TOGAF 9 (The Open Group Architecture Framework)	Enterprise Architecture
17.	United Kingdom Office of Government Commerce's Portfolio, Programme and Project Management Maturity Model (P3M3)	A de facto international standard for integrated ICT portfolio, programme and project management, of which PRINCE2 forms a part for project management.

In terms of the IT Processes prescribed by the CGICTPF the following related standards are applicable:

Table 16: Related Standards in support of the CGICTPF

IT Process reference	Related Standard
EDM01	a) Committee of Sponsoring Organizations of the Treadway Commission (COSO) b) ISO/IEC 38500 c) King III <ul style="list-style-type: none"> • 5.1. The board should be responsible for information technology (IT) governance. • 5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework. d) Organisation for Economic Co-operation and Development (OECD) <ul style="list-style-type: none"> • Corporate Governance Principles
APO01	a) ISO/IEC 20000 <ul style="list-style-type: none"> • 3.1 Management responsibility • 4.4 Continual improvement b) ISO/IEC 27002 <ul style="list-style-type: none"> • 6. Organisation of Information Security c) ITIL V3 2011 Continual Service Improvement, <ul style="list-style-type: none"> • 4.1 The 7-Step Improvement Process
APO02	a) ISO/IEC 20000 <ul style="list-style-type: none"> • 4.0 Planning and implementing service management • 5.0 Planning and implementing new or changed services b) ITIL V3 2011 Service Strategy, <ul style="list-style-type: none"> • 4.1 Strategy Management for IT Services
APO03	a) TOGAF 9 At the core of TOGAF is the Architecture Development Method (ADM), which maps to the COBIT 5 practices of developing an architecture vision (ADM Phase A), defining reference architectures (ADM Phases B,C,D), selecting opportunities and solutions (ADM Phase E), and defining architecture implementation (ADM Phases F, G). A number of TOGAF components map to the COBIT 5 practice of providing enterprise architecture services. These include ADM Requirements Management, Architecture Principles, Stakeholder Management, Business Transformation Readiness Assessment, Risk Management, Capability-Based Planning, Architecture Compliance and Architecture Contracts.
APO05	a) ISO/IEC 20000 <ul style="list-style-type: none"> • 3.1 Management responsibility • 4.0 Planning and implementing service management • 5.0 Planning and implementing new or changed services b) ITIL V3 2011 Service Strategy, <ul style="list-style-type: none"> • 4.2 Service Portfolio Management c) Skills Framework for the Information Age (SFIA)
APO10	a) ISO/IEC 20000 <ul style="list-style-type: none"> • 7.3 Supplier management b) ITIL V3 2011 <ul style="list-style-type: none"> • Service Design, 4.8 Supplier Management

IT Process reference	Related Standard
	c) Project Management Body of Knowledge (PMBOK) <ul style="list-style-type: none"> • PMBOK's procurement processes
APO12	a) ISO/IEC 27001:2005 <ul style="list-style-type: none"> • Information security management systems—Requirements, Section 4 b) ISO/IEC 27002:2011 c) ISO/IEC 31000 <ul style="list-style-type: none"> • 6. Processes for Managing Risk
APO13	a) ISO/IEC 27001:2005 <ul style="list-style-type: none"> • Information security management systems—Requirements, Section 4 b) ISO/IEC 27002:2011 c) National Institute of Standards and Technology (NIST) SP800-53 Rev 1 <ul style="list-style-type: none"> • Recommended Security Controls for USA Federal Information Systems d) ITIL V3 2011 <ul style="list-style-type: none"> • Service Design, 4.7 Information Security Management
BAI01	a) PMBOK b) PRINCE2
DSS01	a) ITIL V3 2011 <ul style="list-style-type: none"> • Service Operation, 4.1 Event Management
DSS04	a) BS 25999:2007 <ul style="list-style-type: none"> • Business Continuity Standard b) ISO/IEC 20000 <ul style="list-style-type: none"> • 6.3 Service continuity and availability management c) ISO/IEC 27002:2011 <ul style="list-style-type: none"> • 14. Business Continuity Management d) ITIL V3 2011 <ul style="list-style-type: none"> • Service Design, 4.6 IT Service Continuity Management
DSS05	a) ISO/IEC 27002:2011 <ul style="list-style-type: none"> • Code of practice for information security management b) NIST SP800-53 Rev 1 <ul style="list-style-type: none"> • Recommended Security Controls for USA Federal Information Systems c) ITIL V3 2011 <ul style="list-style-type: none"> • Service Operation, 4.5 Access Management
MEA01	a) ISO/IEC 20000 <ul style="list-style-type: none"> • 6.2 Service reporting b) ITIL V3 2011 <ul style="list-style-type: none"> • Continual Service Improvement, 4.1 The 7-Step Improvement Process

9.2.4.6.3.4 Principle 4: Enabling a Holistic Approach

Governance and management of enterprise IT must be based on a holistic approach, taking into account interacting components.

COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.

Refer 9.2.4.6.4 COBIT 5 Enablers below for more information.

9.2.4.6.3.5 Principle 5: Separating Governance from Management

Governance and management of ICT must be split.

Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Management is responsible for planning, building, running and monitoring activities in alignment with the direction set by the governance body to achieve LPA objectives.

9.2.4.6.4 COBIT 5 Enablers

Enablers are factors that, individually and collectively, influence whether governance and management over enterprise IT, will successfully function. All enablers need the input of other enablers to be fully effective (e.g. processes need information, organisational structures need skills and behaviour.) All enablers deliver output to the benefit of other enablers (e.g. processes deliver information, skills and; behaviour make processes efficient).

The COBIT 5 framework describes seven categories of enablers (refer figure 5):

- a. **Principles, policies and frameworks** are the vehicle to translate the desired behaviour into practical guidance for day-to-day management. Typical Work Products (WP) in support of this enabler include:
 - I. Enterprise governance guiding principles
 - II. IT-related policies
 - III. IT management framework
 - IV. Decision-making model
 - V. Authority levels
 - VI. Enterprise governance communications
 - VII. Reward system approach
 - VIII. Feedback on governance effectiveness and performance
- b. **Processes** describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals. Typical WP's in support of this enabler include Process Architecture Models.
- c. **Organisational structures** are the key decision-making entities in an enterprise. Typical WP's in support of this enabler include:
 - I. Evaluation of options for IT organisation
 - II. Defined operational placement of IT function
 - III. Definition of organisation structure and functions
 - IV. Organisation operational guidelines
- d. **Culture, ethics and behaviour** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities. Typical WP's in support of this enabler include:
 - I. Ethics charter
 - II. Non-compliance remedial actions
 - III. Communication ground rules
 - IV. Definition of IT-related roles and responsibilities
 - V. Definition of supervisory practices
 - VI. Performance goals and metrics for process improvement tracking
 - VII. Communications on IT objectives
 - VIII. Data classification guidelines
 - IX. Data security and control guidelines
 - X. Data integrity procedures
- e. **Information** is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself. Typical WP's in support of this enabler include Information architecture models.
- f. **Services, infrastructure and applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services. Typical WP's in support of this enabler include:
 - I. Architecture concept business case and value proposition
 - II. Baseline domain descriptions and architecture definition
- g. **People, skills and competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions. Typical WP's in support of this enabler include:
 - I. Competency and career development plans
 - II. Personnel sourcing plans
 - III. Skills and competencies matrix
 - IV. Skills development plans

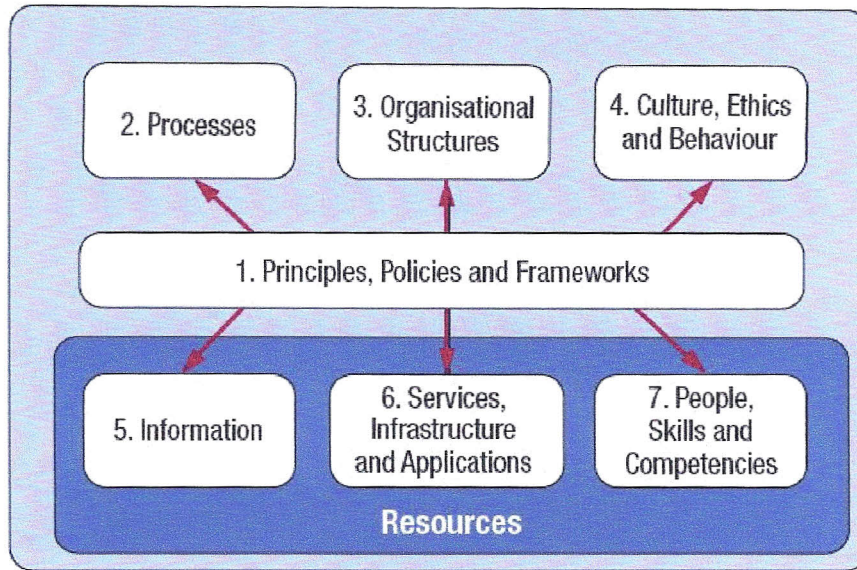


Figure 6: COBIT 5 Enablers

In conclusion it needs to be noted that in order to take the correct decisions the systemic nature of governance and management arrangements must be taken into account. All stakeholder needs must be dealt with by analysing these enablers for relevance and addressing them if required.

Please refer Table 10: Corporate Governance of ICT Policy Framework for a mapping of these enablers to COBIT 5 Process references as incorporated in the CGICTPF.

10 IT Governance Drivers

The LPA has decided to adopt the SITA Change Management process. Permission will be requested from SITA.

Refer Annex F: Change Management Methodology for more details.

11 Information and Communication Technology Corporate Governance of ICT and Governance of ICT RACI Chart

The table below depicts or illustrates who are Responsible, Accountable, Consulted and Informed within the LPA.

Table 17: CGICTPF and CICTF RACI

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
1	Establishment of an ICT Strategic Committee consisting amongst others of members of the Executive Management, the designated Governance Champion and the GTO	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv)	A	R	C	C	I		C								I	I	I	I
2	Chairing by the Accounting Officer of the ICT Strategic Committee to ensure that it is functional	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv)	A, R	I		I			I										I	I
3	Establishment of an ICT Steering Committee consisting of the designated Governance Champion, representatives of strategic business units, the GTO and some members of the Executive Management	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv)	A	R	I	C	I										I	I	I	I
4	Chairing of the ICT Steering Committee by a member of the ICT Strategic Committee to ensure that it is functional	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv)	A	R	C	C		I									I			

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
5	Establishment of an ICT Operational Committee	Public Service Corporate Governance of ICT Policy Framework Implementation Guideline Paragraph 9.2.1	A	C		R	I	I									I			
6	Chairing by the GTO of the ICT operational committee to ensure that it is functional	Public Service Corporate Governance of ICT Policy Framework Implementation Guideline Paragraph 9.2.1	A	C		R		I									I			
7	Establishment of a GITO function	Directive dated 1 February 2005 of the Minister of Public Service and Administration emanating from a national Cabinet Memo 38A of 2000; Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c)(vi)	A R	C	C		C										C	C	I	C
8	Appointment of a proficient GITO for the strategic management of the GITO function	Directive dated 1 February 2005 of the Minister of Public Service and Administration emanating from a national Cabinet Memo 38A of 2000; Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c)(vi)	A	I		C	I			R							C			C
9	Appointment of a proficient ICT manager that supports the GITO	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (vi)	A			C				R							I			

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
10	Designation of a governance champion to drive corporate governance of ICT and the reflection of this responsibility in his/her job description	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (vi)	A, R			I											I			C
11	Designation of an enterprise architect entrusted with the responsibility of defining and maintaining the business architecture of the department	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (vi)	A, R	I		I		I									I			C
12	Establishment of an information systems security office/function that operates independently of the ICT management function	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (vii), (viii) & (ix) & COBIT Process APO13	A	C	C	C	C		R								C			C
13	Ensuring that the GITO is a member of the Executive Management (and of the ICT Strategic Committee in the case whereby the Executive Management does not dovetail as the ICT Strategic Committee)	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv) & (vi)	A, R	I		C			I								I			
14	Ensuring that the designated Governance Champion reports to the Executive Management and is a member of the ICT Strategic Committee	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv) & (vi)	A, R	I				I	I								I			
15	Ensuring that the designated Governance Champion is a member of the ICT Strategic Committee	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv) & (vi)	A, R	I					I								I			

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
16	Establishment of an ICT strategic plan (ICT plan or strategic information systems plan or master systems plan) that is no more than three years old in terms of recency and that is commensurate with the business strategic plan exists and is approved and the former supports the latter	Public Service Corporate Governance of ICT Policy Framework 20.6 (b), 20.9 (b) (i), Implementation Guideline Paragraphs 10, 10.1 & COBIT Process APO02	A		C	R		I	C	C	C						C			C
17	Approval of an ICT strategic plan (ICT plan or strategic information systems plan or master systems plan)	Public Service Corporate Governance of ICT Policy Framework 20.6 (b), 20.9 (b) (i), Implementation Guideline Paragraphs 10, 10.1 & COBIT Process APO02	A, R		I						I						I			C
18	Establishment of a defined and documented enterprise business architecture that includes an information architecture of the department exists	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (i), 20.9 (b) (ii), Implementation Guideline Paragraph 10.4 & COBIT Process APO03	A	C	R	C	C		C		C						C	I	C	C
19	Definition and documentation of the ICT architecture of the department that consists of an information systems architecture and a technology architecture is defined and documented as a subset of the enterprise business architecture of the department, and ensuring that the former supports the latter	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (ii), 20.6 (b) Implementation Guideline Paragraph 10.4 & COBIT Process APO03	A		C	R		C	C	C							C	I		

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
20	Establishment of an ICT migration and/or architecture migration plan from the as-is situation or architecture to the to-be situation or architecture exists, is approved and current	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (ii), 20.6 (b), 20.9 (b) (iii), Implementation Guideline Paragraph 10.4 & COBIT Process APO03	A		I	R		C	C	C	I						C	I		
21	Establishment of a business disaster recovery and continuity plan of the department	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (x) & COBIT Process DSS04	A	I	I	C	C		C	R	I								C	C
22	Approval of a business disaster recovery and continuity plan of the department	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (x) & COBIT Process DSS04	A R	I	I	I	I		I		I						I	I		C
23	Establishment of an ICT service disaster recovery and continuity plan as a subset of the business disaster recovery and continuity plan of the department, and ensuring that the former supports the latter.	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (x) & COBIT Process DSS04	A		C	R		C	C	C	C						C	I		I
24	Approval of an ICT service disaster recovery and continuity plan as a subset of the business disaster recovery and continuity plan of the department, and ensuring that the former supports the latter	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (x) & COBIT Process DSS04	A R		I	I		I	I	I	I						I	I		C
25	Establishment of an Annual Performance Plan (APP) that includes an ICT implementation plan (ICT Annual Performance Plan for 2015-2016 and onwards)	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.6 (b), 20.9 (b) (v) & Implementation Guideline Paragraph 10.2	A		C	C	C		C		R						I	C	I	C

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
26	Approval of an Annual Performance Plan (APP) that includes an ICT implementation plan (ICT Annual Performance Plan for 2015-2016 and onwards)	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.6 (b), 20.9 (b) (v) & Implementation Guideline Paragraph 10.2	A R	I	I	I	I	I	I	I	I						I	I	I	C
27	Establishment of an ICT operational plan for a current financial year	Public Service Corporate Governance of ICT Policy Framework Implementation Guideline Paragraphs 9.2.2.1 & 10.3 and COBIT Process DSS01				A C	I	R		I	I									
28	Approval of an ICT operational plan for a current financial year	Public Service Corporate Governance of ICT Policy Framework Implementation Guideline Paragraphs 9.2.2.1 & 10.3 and COBIT Process DSS01	A			C	C	I		C	R									
29	Establishment of an ICT procurement strategy that adheres to the ICT House of Value and that takes into consideration SITA General Regulations of 2005	Public Service Corporate Governance of ICT Policy Framework 20.9 (b) (iv) and COBIT Processes APO02 & APO10	A			R	C	C		C	C						I			
30	Approval of an ICT procurement strategy that adheres to the ICT House of Value and that takes into consideration SITA General Regulations of 2005	Public Service Corporate Governance of ICT Policy Framework 20.9 (b) (iv) and COBIT Processes APO02 & APO10	A R				C			C	C						I			C
31	Establishment of an ICT procurement plan for a current financial year that is in line with the approved ICT procurement strategy	Public Service Corporate Governance of ICT Policy Framework 20.9 (b) (iv) and COBIT Processes APO02 & APO10	A			C	C	R	C	C	C						I			

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
32	Approval of an ICT procurement plan for the current financial year that is in line with the approved ICT procurement strategy	Public Service Corporate Governance of ICT Policy Framework 20.9 (b) (iv) and COBIT Processes APO02 & APO10	A R			I	I	I	I	I							I			C
33	Establishment of a corporate governance of ICT policy/framework	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (a) and COBIT Process EDM01	A	C	C	R	C	C	C	C	C						C	I	C	C
34	Approval of a corporate governance of ICT policy/framework	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (a) and COBIT Process EDM01	A R	I	I	I	I	I	I	I	I						I	I	I	C
35	Ensuring the implementation of a corporate governance of ICT policy/framework exists and is approved	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (a) and COBIT Process EDM01	A	R				I									I			
36	Establishment of a governance of ICT framework/policy/charter	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (b) and (c) and COBIT Process EDM01	A	C	C	R		C	C	C							C			I
37	Approval of a governance of ICT framework/policy/charter	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (b) and (c) and COBIT Process EDM01	A R	I	I	I	I	I	I	I	I						I			C
38	Ensuring the implementation of a governance of ICT framework/policy/charter	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (b) and (c) and COBIT Process EDM01	A	C		R		C									I			
39	Establishment of an ICT risk register that denotes strategic ICT risks and operational ICT risks	National Treasury Risk Management Framework and COBIT Processes EDM03 & APO12	A			R		C				C					I			

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
40	Updating of the ICT risk register that denotes strategic ICT risks and operational ICT risks every financial year	National Treasury Risk Management Framework and COBIT Processes EDM03 & APO12	A			R		C				C					I			
41	Establishment of an ICT security strategy, policy and implementation plan	Public Service Corporate Governance of ICT Policy Framework 20.5 (d) (ix), 20.9 (a) (vii), Implementation Guideline Paragraph 9.4 and COBIT Processes APO13 & DSS05	A			R		C				C					C	I		
42	Approval of an ICT security strategy, policy and implementation plan	Public Service Corporate Governance of ICT Policy Framework 20.5 (d) (ix), 20.9 (a) (vii), Implementation Guideline Paragraph 9.4 and COBIT Processes APO13 & DSS05	A R			I	I	I	I			I					I			C
43	Implementation of the approved ICT security strategy and policy and execution of the implementation plan	Public Service Corporate Governance of ICT Policy Framework 20.5 (d) (ix), 20.9 (a) (vii), Implementation Guideline Paragraph 9.4 and COBIT Processes APO13 & DSS05	A			R	R	R	R	R		C					I			I
44	Establishment of an ICT portfolio management framework/methodology based on an internationally accepted framework/methodology	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (vi), 20.9 (a) (vii) and COBIT Processes APO05 and BAI01	A		C	R		C									C			
45	Approval of an ICT portfolio management framework/methodology based on an internationally accepted framework/methodology	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (vi), 20.9 (a) (vii) and COBIT Processes APO05 and BAI01	A R		I	I		I	I	I		I					I			C

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
46	Implementation of the approved ICT portfolio management framework/methodology based on an internationally accepted framework/methodology	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (vi), 20.9 (a) (vii) and COBIT Processes APC05 and BAI01	A			R	R	R	R	R							I			
47	Establishment of an ICT management framework/methodology used to manage the ICT function.	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (v), 20.9 (a) (vi) and COBIT Process APC01	A			R		C		C							C			
48	Approval of an ICT management framework/methodology used to manage the ICT function.	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (v), 20.9 (a) (vi) and COBIT Process APC01	A R	I		I	I	I	I	I		I					I			C
49	Ensuring the implementation of the approved ICT management framework/methodology used to manage the ICT function	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) (v), 20.9 (a) (vi) and COBIT Process APC01	A			R	R	R	R			R					I			
50	Establishment of a change management plan that addresses human behavioural and cultural aspects to ensure a smooth transition from the as-is situation to the to-be situation by the political and strategic management leadership right down to the operational staff and that includes training, communication, organisational redesign and process redesign exists	Public Service Corporate Governance of ICT Policy Framework Implementation Guideline Paragraph 9.4 and COBIT Processes BAI05, BAI06 & BAI07	A			R	C	R	C	C	C						C			

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
51	Implementation of the change management plan that addresses human behavioural and cultural aspects to ensure a smooth transition from the as-is situation to the to-be situation by the political and strategic management leadership right down to the operational staff and that includes training, communication, organisational redesign and process redesign exists	Public Service Corporate Governance of ICT Policy Framework Implementation Guideline Paragraph 9.4 and COBIT Processes BAI05, BAI06 & BAI07	A			R	R	R	R	R	C						I			
52	Establishment of a roadmap for the continuous improvement of the states or levels of maturity of the Corporate Governance of ICT and of the Governance of ICT as well as the improvement of the alignment of ICT service provision with business aspirations and of the support ICT delivers to business	Public Service Corporate Governance of ICT Policy Framework 20.7 and 20.9 (c), Implementation Guideline Paragraphs 6 and 11 and COBIT Processes EDM02 & MEA01	A	R	R	R		R	R	R	C	C					C			I
53	Approval of the roadmap for the continuous improvement of the states or levels of maturity of the Corporate Governance of ICT and of the Governance of ICT as well as the improvement of the alignment of ICT service provision with business aspirations and of the support ICT delivers to business	Public Service Corporate Governance of ICT Policy Framework 20.7 and 20.9 (c), Implementation Guideline Paragraphs 6 and 11 and COBIT Processes EDM02 & MEA01	A, R	I	I	I	I	I	I	I	I	I					I			C

CONFIDENTIAL

No.	Compliance Requirement / Performance Standard/Target	Compliance Mandate / Source of Authority (Act / Regulation / Policy / Agreement / Ministerial Directive / Standard) &/or Reference Number	Head of Department	Governance Champion	Enterprise Architect	Departmental Government IT Officer	Chief Financial Officer	ICT Manager	Strategic Business Unit Managers	Head: Corporate Services	Head: Strategic Planning	Head: Risk Management	Head: Legal Services	ICT Strategic Committee	ICT Steering Committee	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Institutional Support	Director-General	Executing Authority
54	Implementation of the approved roadmap for the continuous improvement of the states or levels of maturity of the Corporate Governance of ICT and of the Governance of ICT as well as the improvement of the alignment of ICT service provision with business aspirations and of the support ICT delivers to business	Public Service Corporate Governance of ICT Policy Framework 20.7 and 20.9 (c), Implementation Guideline Paragraphs 6 and 11 and COBIT Processes EDM02 & MEA01	A	R	R	R	R	R	R	R	C	C					I			I
55	Establishment of a business agreement with SITA to govern the relationship between SITA and departments	SITA Act, SITA Regulation 5.1.1 and COBIT Process APC08	C			C							C				R		A	I
56	Approval of a business agreement with SITA to govern the relationship between SITA and departments	SITA Act, SITA Regulation 5.1.1 and COBIT Process APC08	I	I		I	I	I		I			C				I		AR	C
57	Co-signing of a business agreement with SITA to govern the relationship between SITA and a department	SITA Act, SITA Regulation 5.1.1 and COBIT Process APC08	R	I		I	I	I		I			C				I		AR	I
58	Services acquired or to be acquired from SITA are listed in an appendix to the business agreement entered into with SITA	SITA Act, SITA Regulation 5.1.3 and COBIT Process APC09	A			R	C	R									R			
59	Establishment of a service level agreement in respect of each and every ICT service obtained from a service provider/s, including SITA.	SITA Act, SITA Business Agreement & COBIT Processes APC09 & APC10	A			R	C	R	I	I		C	C				C			