LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
EDUCATION

FRAMEWORK, CHARTER AND CONTINUOUS IMPROVEMENT ROADMAP

Limpopo Department Of Education Governance of ICT Framework (GICTF), Charter and Improvement Roadmap

VERSION	**1.0**
DATE	**10 October 2013**

APPROVAL PAGE:

LIMPOPO DEPARTMENT OF EDUCATION GOVERNANCE OF ICT FRAMEWORK (GICTF), CHARTER AND IMPROVEMENT ROADMAP

Approved/ ~~Not Approved~~

Mrs. O Dederen
Acting Head of Department

Date : 25/11/2013

TABLE OF CONTENTS

TABLE OF CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

The main objective of this document is to depicts the IT governance capability maturity status for the Limpopo department of education as derived from the IT governance capability maturity assessments conducted by SITA for Limpopo provincial departments, and outline the department ‘s corporate governance framework of ICT policy framework charter and improvement roadmap.

This document will also recommended IT Governance Framework, charter and the implementation roadmap for the department.

This document utilizes information referenced from the following sources:-

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

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®.

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 department, “the board” as mentioned above, refers to the Executive Management Committee (EMC).

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 department 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 Limpopo provincial administration 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 departments 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 provincial 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,

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

k. Department of Economic Development, Environment & Tourism,
l. Department of Roads and Transport (in 2011) and
m. The Office of the Premier.

This document must be read in conjunction with the CGICTPF (corporate governance of ICT policy framework, as adapted by the department.

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 department 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 including Limpopo department of education 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 D: 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.

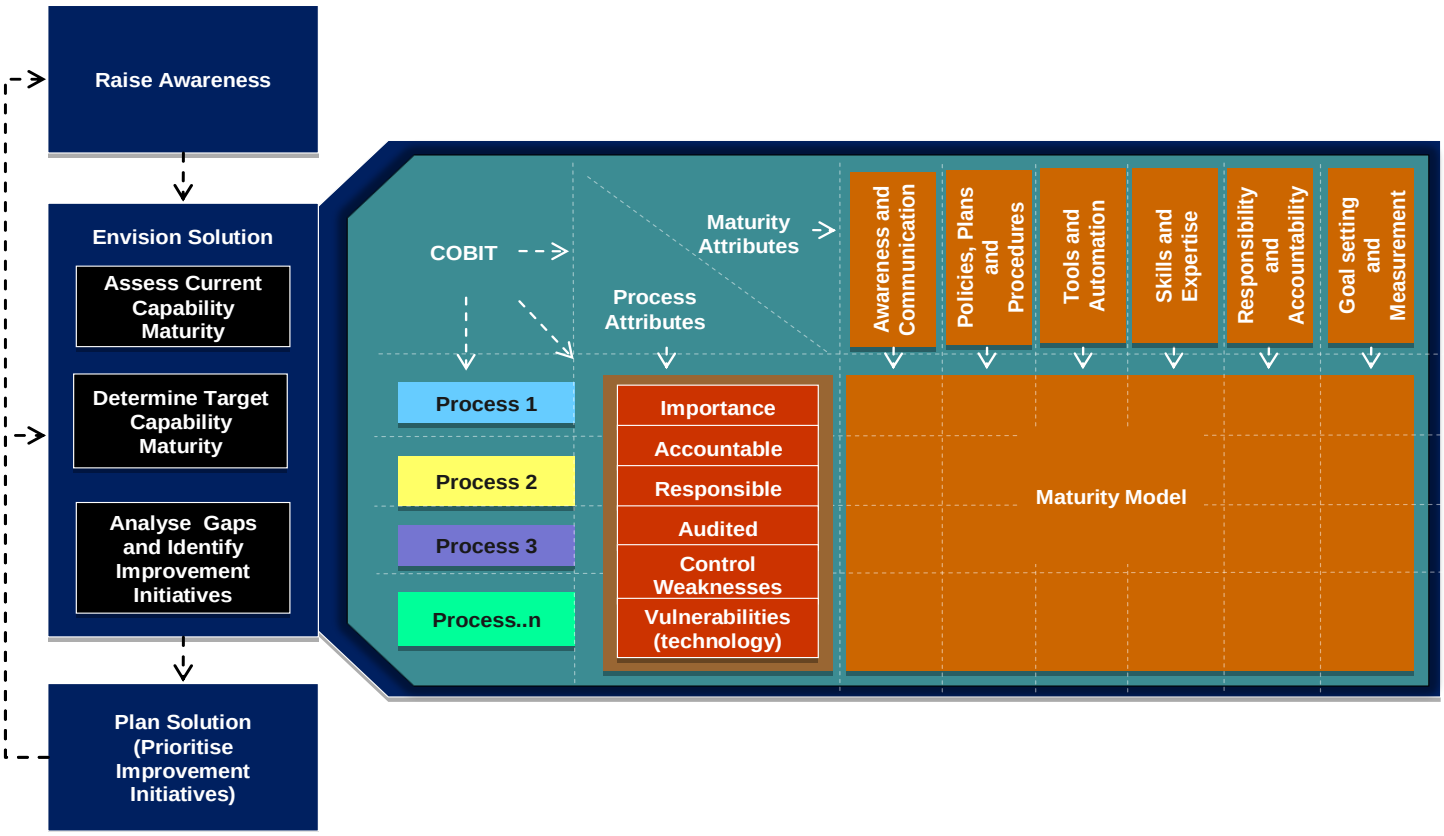


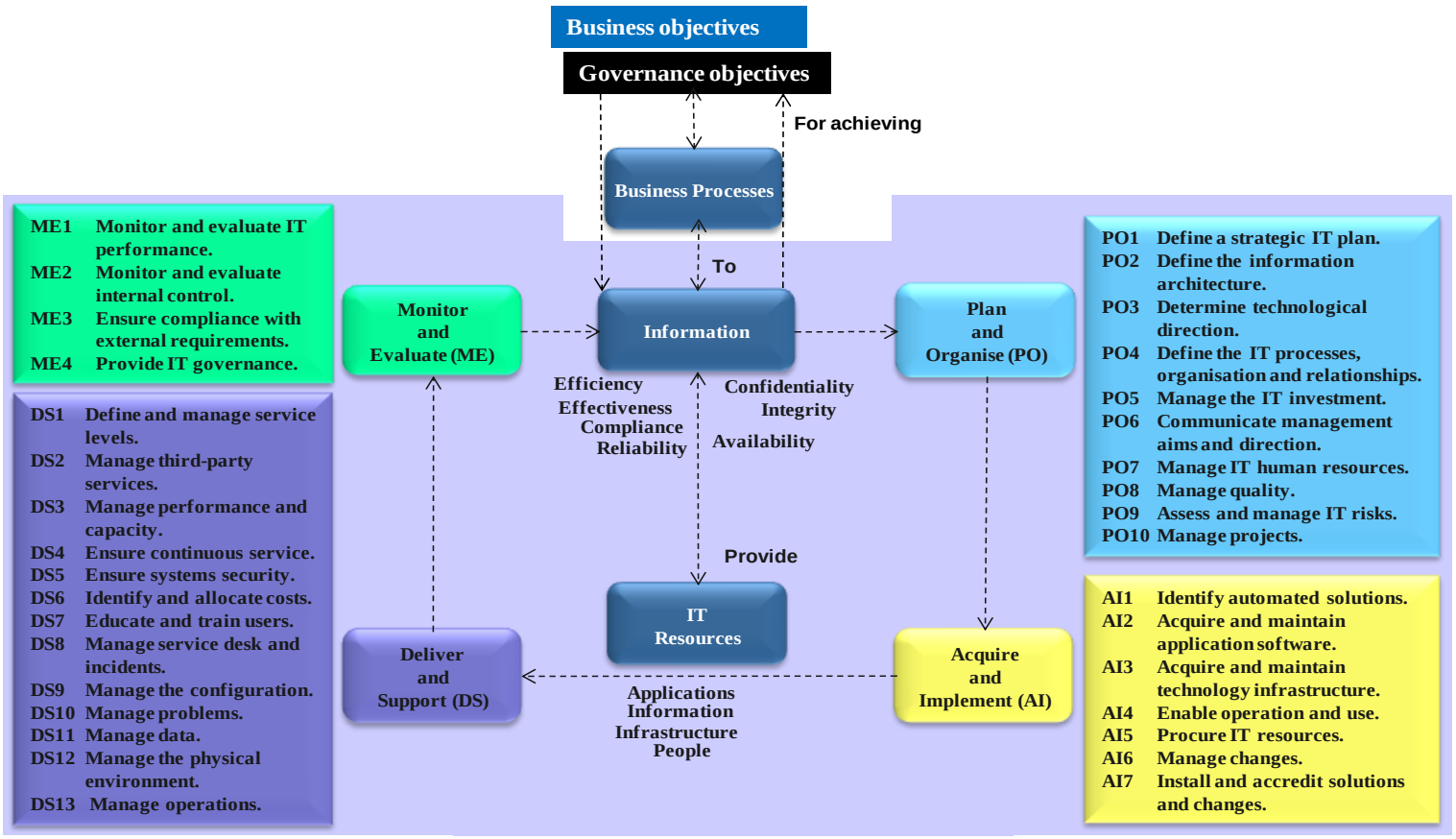
Figure 1: IT Governance Capability Maturity Assessment Framework

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 0 Overview of COBIT 4.1 Domains and IT Processes.

6 Project Scope

6.1 Inclusions

a) The audit report for the department were studied, analysed and incorporated into the respective departmental report, and
b) Facilitation of the ICT governance capability assessment, and development of ICT Governance framework and charter & improvement roadmap for the department using the SITA ICT governance capability maturity assessment framework.

6.2 Exclusions

a) assessment of the additional COBIT 5 processes which extend beyond COBIT 4.1,
b) detailed analysis of existing IT policies, procedures and processes,
c) development of IT related policies, procedures, processes or standards,
d) procurement of hardware and software,
e) analysis of Government legislation and regulations,
f) analysis of business policies, procedures and processes, and
g) Provision or procurement of any information systems through this project.

7 IT Governance Drivers

The department 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

Category	Description
Acts and regulations	a) Public Service Act, 1994 b) Preferential Procurement Policy Framework Act No 5 of. 2000, c) The Electronic Communications and Transactions Act (Act. No. 25 of 2002), d) Public Service Regulations 2001, as amended 28 April 2006, • 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.

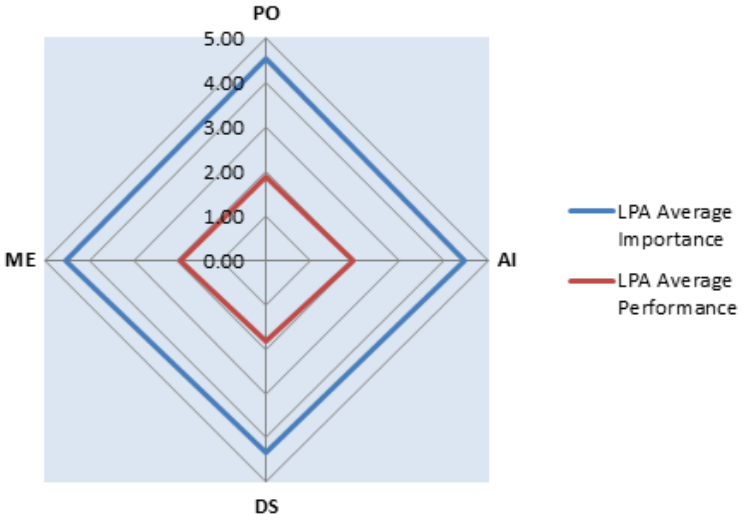


Figure 3: Limpopo department of education Assessment Results per ITS Domain

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: Limpopo department of education Assessment Results per ITS Domain

Description	PO	AI	DS	ME	Average
Average Importance	4.52	4.45	4.32	4.53	4.45
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 D: Rating Scales.

8.1.2 Selected IT Processes for the Limpopo department of education

Based on the assessments conducted by SITA for the department, 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 Accredit 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 department is going to utilise in the execution of its IT governance activities.

This framework will also touch on addressing:
a) The department ‘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 Auditor General Findings.

9.2 ICT Governance Framework Contents

9.2.1 ICT Governance Principles and Practices

For the principles, practices and objectives applicable to the department, as per the CGICTF, refer to Annex B: 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 0 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 department. It includes a framework, policies, processes, policies, plans, procedures, decision and reporting structures for ICT and accountability structures.

Table 4: Limpopo department of education ICT Governance Framework based on COBIT 4.1

IT Governance Framework for the Department	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, P010.5, PO10.7, PO10.10	AI2.1, AI2.2, AI2.8, AI2.10, AI6.4, AI7.1, AI7.2, AI7.3, AI7.9,	DS4.2	
	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	ICT Sub Branch (GITO) (Head of Department)	Head of Department	Head of Department	Head of Department
	Responsibility Structures	The department	The department	The department	The department

Refer Annex C: Limpopo department of education ICT Framework-, Processes-, Plans-, Procedures- and Policies Framework for a full depiction of the target department environment.

Table 5: Limpopo department of education ICT Governance Framework based on COBIT 4.1 mapped to COBIT 5

IT Governance Framework for the Department	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, 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	BAI03.01, BAI03.02, BAI03.06, BAI03.10, BAI06.03, BAI05.05, BAI07.01, BAI07.03, BAI07.01, BAI07.08	DSS04.03	
	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,	DSS04.01 DSS04.02, DSS04.03, DSS04.04, DSS04.06, DSS04.09, DSS02.04, DSS02.05 DSS02.06,	

IT Governance	Category	Align, Plan and Organize (APO)	Build, Acquire and Implement (BAI)	Deliver, Service and Support (DSS)	Monitor, Evaluate and Assess (MEA)
			BAI07.08	BAI10.03, DSS03.02, DSS03.03, DSS03.04	
	Decision Reporting and structures for IT decisions	APO01.01			EDM01.01
	Accountability Structures	ICT sub branch (GITO) (Head of Department)	Head of Department	Head of Department	Head of Department
	Responsibility Structures	The department	The department	The department	The department

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 Corporate governance of ICT policy framework charter

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

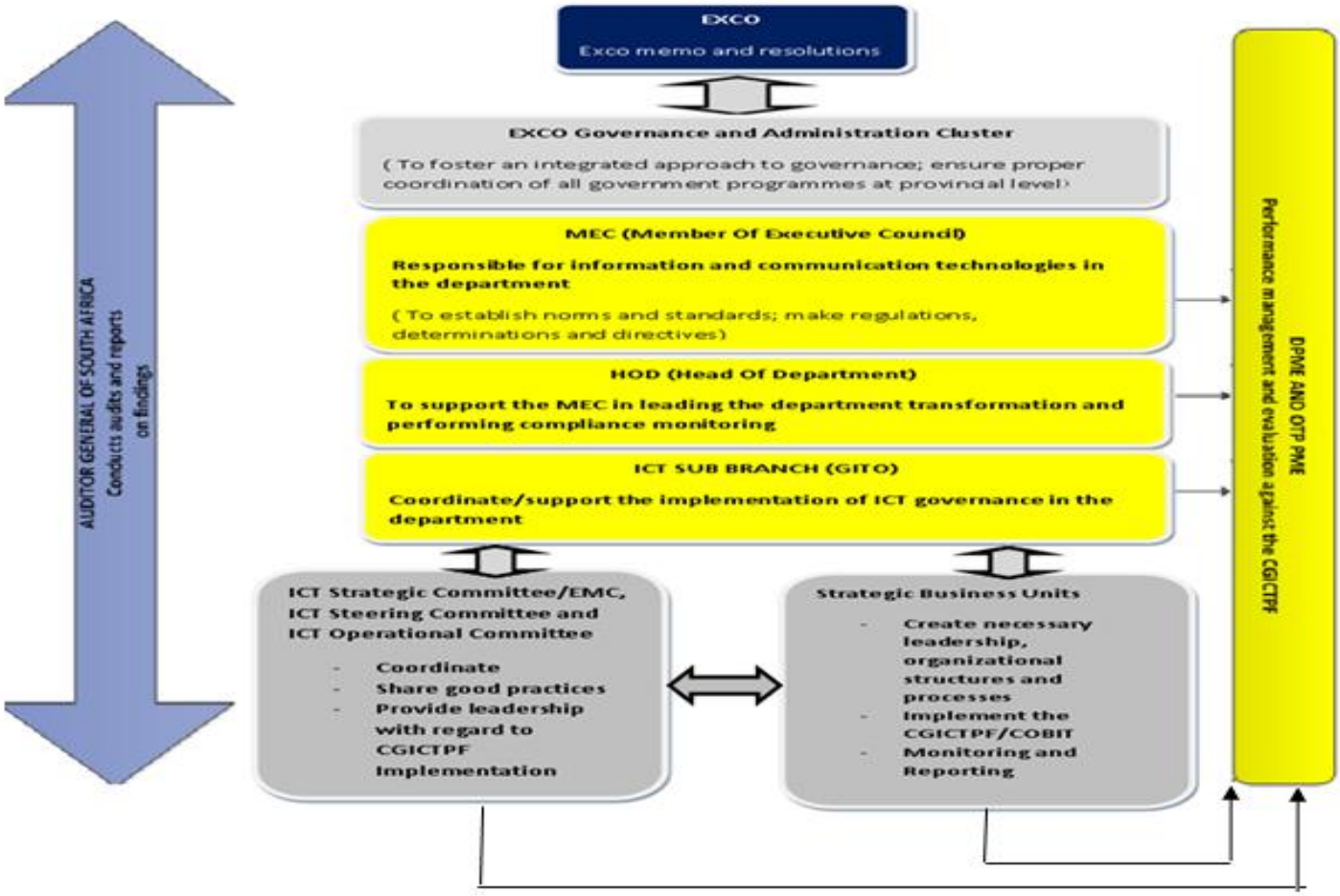


Figure 4: Governance Structures for the Limpopo department of education

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

9.2.3.1 ICT Strategic Committee (incorporated into EMC – Executive Management 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 ICT Strategic Committee was incorporated into EMC (executive management committee) chaired by the accounting officer/ head of department, in the Limpopo department of education.

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

Table 6: ICT Strategic Committee Responsibilities

Responsibilities			Chairperson / Members
Evaluate	**Conceptualise and direct**	**Monitor**	
Evaluate the departmental strategic plan, internal and external environment to:	Conceptualise and direct business enablement by ICT arrangements:	**Monitor** that implementation conforms to the criteria:	**Chair:** Accounting officer/Head of department **Members:** Executive Management/Senior General Managers, the Governance Champion (GC) and Enterprise Architect.
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 monitor significant ICT expenditure	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	a) Conformance, performance and assurance oversight and monitoring b) Ensure that risk is managed and the ICT is audited internally and independently	

Responsibilities			Chairperson / Members
Evaluate	**Conceptualise and direct**	**Monitor**	
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 blow 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	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	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	**Chair:** Member of EMC (Executive Management Committee) **Members:** Executive and Senior Management, the Governance Champion (GC), Enterprise Architect and GITO.

Responsibilities			Chairperson / Members
Evaluate:	**Direct:**	**Monitor:**	
Committee and/or HoD d) Oversee the identification of the ICT prescriptive environment	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		

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 blow 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 and ICT management.

9.2.3.4 Audit and Risk Committee

This committee reports on the adequacy of controls in the department.
The table blow 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	**Chairperson**: Audit / Risk **Members:** Business and ICT

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	

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.

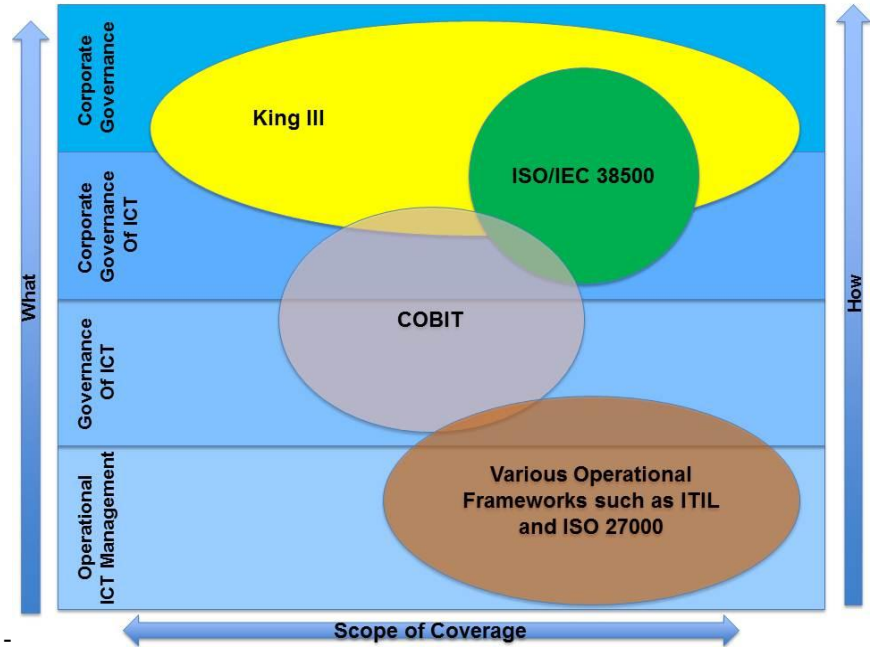


Figure 5: Interrelation of these different Frameworks and Standards

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 process(es). Also included is a depicting of the COBIT 7, 7 enablers mapped to the relevant IT process reference.

Table 10: Corporate Governance of ICT Policy Framework

IT Governance Framework for the Department	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	Limpopo department of education 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	Limpopo department of education 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												

IT Governance	Category	Deliverable / Enabler	EDM	APO						BAI	DSS				MEA	CGICTPF
			EDM01	APO01	APO02	APO03	APO05	APO10	APO12	APO13	BAI01	DSS01	DSS04	DSS05	MEA01	
		Information				X										
		Services, infrastructure and applications				X										
		People, skills and competencies (not part of the CGICTPF): APO07														

The ICT plans, ICT implementation plans and ICT operational plans have been replaced with Enterprise Architecture, based on GWEA (government wide enterprise architecture).

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), Limpopo office of the premier 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 department will be operating the following frameworks. These frameworks are as a result of the IT Capability Maturity assessment that was conducted by SITA and 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 department 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 the Projects 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 department ICT Governance Framework includes a process framework, and it includes processes as indicated as part of Annex C: Limpopo department of education 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	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.
	AI7.8	BAI07.06	An approval process for application, system and configuration transfer from testing to the production environment exists.

Domain	ICT Processes		
	Control Objective	**COBIT 5 Process Reference**	**IT Process Description**
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; DSS02.06	A process to manage the resolution and closure of each incident, 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 department.

9.2.4.5 Plans

The department 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 department 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 department 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			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; APO02.04; APO02.05; APO04.03; APO04.04; APO04.05	Technology Infrastructure Plan
	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 ICT sub branch (GITO) in the department 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			Policy
	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 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 department's ICT Governance Framework.

Table 14: Required IT Procedures

Domain			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	NA

Domain		Procedures	
	Control Objective Reference	COBIT 5 Process Reference	Name and/or Description
		Desk as a process.	
	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;DSS02.06	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.
	DS10.3	DSS03.03;DSS03.04	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 department to create an effective governance and management framework in order to optimise information and technology investments to the benefit of stakeholders. Also refer Annex B: ICT Governance Principles, Practices and Objectives as has been adopted by the department.

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 department; 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 department.
b. It considers all IT-related governance and management enablers to be department 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

#	Standard	Description
8.	ISO/IEC 9001	Quality management systems
9.	King III	Corporate and IT Governance
10.	NA	Kotter, John; *Leading Change*, 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 environments, version 2)	Project Management
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 • 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) • Corporate Governance Principles
APO01	a) ISO/IEC 20000 • 3.1 Management responsibility • 4.4 Continual improvement b) ISO/IEC 27002 • 6. Organisation of Information Security c) ITIL V3 2011 Continual Service Improvement, • 4.1 The 7-Step Improvement Process
APO02	a) ISO/IEC 20000 • 4.0 Planning and implementing service management • 5.0 Planning and implementing new or changed services b) ITIL V3 2011 Service Strategy, • 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 • 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, • 4.2 Service Portfolio Management c) Skills Framework for the Information Age (SFIA)
APO10	a) ISO/IEC 20000 • 7.3 Supplier management b) ITIL V3 2011

IT Process reference	Related Standard
	• Service Design, 4.8 Supplier Management c) Project Management Body of Knowledge (PMBOK) • PMBOK's procurement processes
APO12	a) ISO/IEC 27001:2005 • Information security management systems—Requirements, Section 4 b) ISO/IEC 27002:2011 c) ISO/IEC 31000 • 6. Processes for Managing Risk
APO13	a) ISO/IEC 27001:2005 • Information security management systems—Requirements, Section 4 b) ISO/IEC 27002:2011 c) National Institute of Standards and Technology (NIST) SP800-53 Rev 1 • Recommended Security Controls for USA Federal Information Systems d) ITIL V3 2011 • Service Design, 4.7 Information Security Management
BAI01	a) PMBOK b) PRINCE2
DSS01	a) ITIL V3 2011 • Service Operation, 4.1 Event Management
DSS04	a) BS 25999:2007 • Business Continuity Standard b) ISO/IEC 20000 • 6.3 Service continuity and availability management c) ISO/IEC 27002:2011 • 14. Business Continuity Management d) ITIL V3 2011 • Service Design, 4.6 IT Service Continuity Management
DSS05	a) ISO/IEC 27002:2011 • Code of practice for information security management b) NIST SP800-53 Rev 1 • Recommended Security Controls for USA Federal Information Systems c) ITIL V3 2011 • Service Operation, 4.5 Access Management
MEA01	a) ISO/IEC 20000 • 6.2 Service reporting b) ITIL V3 2011 • 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 department 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

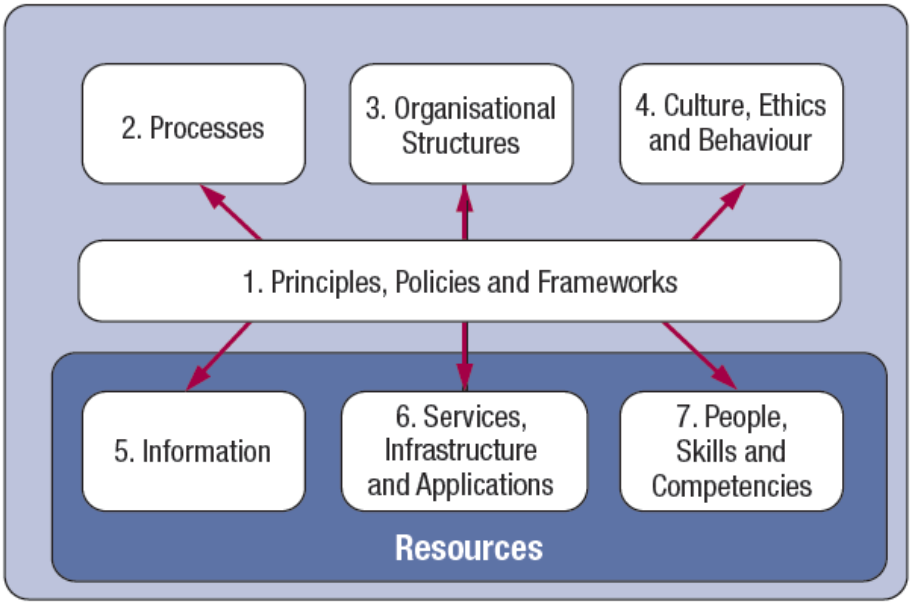


Figure 6: COBIT 5 Enablers

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

The table below depicts illustrates who is Responsible, Accountable, Consulted and Informed within the Limpopo department of department.

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
1	Establishment of an **ICT Strategic Committee** consisting amongst others of members of the Executive Management, the designated Governance Champion and the GITO	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (c) (iv)	A	R	C	C	I		C								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
3	Establishment of an **ICT Steering Committee** consisting of the designated Governance Champion, representatives of strategic business units, the GITO 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

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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		
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 GITO 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	C

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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		
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

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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		

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	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 regency 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

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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	
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
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

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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	C
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	C

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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		

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	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						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
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	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

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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		
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) (viii), 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) (viii), Implementation Guideline Paragraph 9.4 and COBIT Processes APO13 & DSS05	A, R			I	I	I	I			I					I		C

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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) (viii), 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
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 APO05 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 APO01	A			R		C		C							C		

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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 APO01	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 APO01	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		

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	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

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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
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 APO08	C			C							C				R		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 APO08	I	I		I	I	I		I			C				I		C

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
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 APO08	R	I		I	I	I		I			C				I		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 APO09	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 APO09 & APO10	A			R	C	R	I	I		C	C				C		
60	Approvals of service level agreements in respect of each and every ICT service obtained from a service provider/s, including SITA, exist, are signed and are current.	SITA Act, SITA Business Agreement & COBIT Processes APO09 & APO10	A, R			I	I	I	I	I		I	C				I		C
61	Chairing of **service provision or service delivery review meetings** in accordance with the schedule provisions of a service level agreement	SITA Act & SITA Business Agreement & COBIT Processes APO09 & APO10	A			R		R									I		
62	Establishment of an **ICT project charter or project statement of work** in respect of each and every project undertaken or to be undertaken by a service provider.	SITA Business Agreement & COBIT Process BAI01	A			R	C	R	C			C	C				C		

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
63	Approval of an **ICT project charter or project statement of work** in respect of each and every project undertaken or to be undertaken by a service provider.	SITA Business Agreement & COBIT Process BAI01	A, R			I	I	I	I	I		I	C				I		C
64	Ensuring that **ICT projects** executed by a service provider/s are managed in accordance with the provisions of the signed project charter or statements of work	SITA Business Agreement & COBIT Process BAI01	A			R	R	R	R								I		
65	**Participation of the GITO in the Provincial GITO Forum**	Directive dated 1 February 2005 of Minister of Public Service and Administration emanating from a national Cabinet Memo 38A of 2000 and Public Service Corporate Governance of ICT Policy Framework Paragraph 16.1 (b)	A			R		I									R		
66	Establishment of a **software asset register**	COBIT Process BAI09	A			R	C	R									I		
67	Updating of a **software asset register** at least once every financial year	COBIT Process BAI09	A			R	C	R									I		
68	Assessment annually of **business relevance** of software assets	COBIT Process BAI09	A			R	I	R	C								I		

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
69	Negotiation of a **software licence agreement** with a software provider	COBIT Process BAI09	A			R	C	R	C	C		C	C				I		
70	Approval of a **software licence agreement** with software provider	COBIT Process BAI09	A, R			I	I	I	I	I		I	C				I		C
71	Termination of a **software licence agreement** with a software provider that does not grant a user rights of use in perpetuity	COBIT Process BAI09	A			R	C	C		C		C	R				C		I
72	Termination of a **software licence agreement** with a software provider that grants a user rights of use in perpetuity	COBIT Process BAI09	A, R			R	I	I		I		C	R				C		C
73	Ensuring that terms and conditions of **a software licence agreement** are complied with	COBIT Process BAI09	A	I		R		R	R				R						
74	Establishment of **other enabling policies, frameworks, plans and structures**	Public Service Corporate Governance of ICT Policy Framework Paragraph 20.5 (d) & COBIT Processes APO01, APO03, APO05, APO12, APO13, BAI01, DSS01, DSS04 & MEA01	A	R	R	R	C	R	C	C	C						C		C

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
75	Establishment of an **information plan, an information infrastructure plan and an operational plan**	Public Service Regulations Chapter 1 Part II E.1(a), (b) and (c)	A		R	C	C	C	C	C	R						C		C
76	Approval of an **information plan, an information infrastructure plan and an operational plan**	Public Service Regulations Chapter 1 Part II E.1(a), (b) and (c)	A, R	I	I	I	I	I	I	I	I	I	I				I	I	C
77	Ensuring the resourcing (with budget, human resources, facilities, etc.) of the approved **information plan, information infrastructure plan and operational plan**	Public Service Regulations Chapter 1 Part II E.1(a), (b) and (c)	A, R			R	R		C	R	R						I	I	I
78	Ensuring the implementation of the approved **information plan, information infrastructure plan and operational plan**	Public Service Regulations Chapter 1 Part II E.1(a), (b) and (c)	A, R		R	R	R	I	R	R	R						I	I	I
80	**Server backups** are taken on a regular basis (daily, weekly and/or monthly)	COBIT Process DSS04 & DSS05	A			R		R				I							
81	**Desktop backups** are taken on a regular basis (daily, weekly and/or monthly)	COBIT Processes DSS04 and DSS05	A			R		R	I			I							
82	**Backup tapes/data** is stored at an offsite location	COBIT Processes DSS04 and DSS05	A			R		R				I							

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
83	**Backed up data is tested** for restorability and integrity on a regular basis	COBIT Processes DSS04 and DSS05	A			R		R				I							
84	**Patches** of the operating system and other systems software is done consistently and is being managed	COBIT Processes APO12, BAI06, BAI07, BAI10, DSS01, DSS04 and DSS05	A			R		R											
85	The **antivirus facility** is being updated on a regular basis on both servers and user workstations	COBIT Processes APO12, BAI06, BAI07, BAI10, DSS01, DSS04 and DSS05	A			R		R											
86	An **ICT applications user access management policy** exists and is reviewed on a periodic basis	COBIT Process DSS05 APO07, APO13, DSS01 and DSS05	A			R	R	R	R	R									
87	Establishment of an **ICT incident register** that is used to record all ICT incidents as and when they occur	COBIT Processes DSS02 and DSS03	A			C		R											
88	Checking on a regular basis of an **ICT incident register** that is used to record all ICT incidents as and when they occur	COBIT Processes DSS02 and DSS03	A			R		R				I							

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	Senior General Manager: Corporate Services	Senior General Manager : Education Planning	Senior Manager : Risk Management	Senior Manager: Legal Services	ICT Strategic Committee	ICT Steering Committee(incorporated into EMC	ICT Operational Committee	Provincial Government IT Officer	Senior General Manager: Curriculum Delivery Management	Executing Authority
89	Benefits (free training vouchers) ensuing from the Microsoft Enterprise Agreement are utilised or alternatively offered to departments that are in need of them	Microsoft Enterprise Agreement																	

Legend:
Accountable: In a Responsible, Accountable, Consulted, Informed (RACI) chart refers to the person or group who has the authority to approve or accept the execution of an activity.
Responsible: In a RACI chart, refers to the person who must ensure that activities are completed successfully.
Consulted: In a RACI chart, refers to those people whose opinions are sought on an activity (two-way communication).
Informed: In a RACI chart, Informed refers to those people who are kept up to date on the progress of an activity (one-way communication).

11 IT Governance Improvement Roadmap

11.1 Initiative planning

The following table lists the source, action by, due date per initiative and the RACI in terms of accountability and responsibility.

Table 18: Initiative Planning

#	Initiative	Due Date	Comments	Duration in months	Estimated cost	RACI	
						Accountable	Responsible
CGICTPF							
1	Designation of a Governance Champion to coordinate the development and implementation of the CGICT policy	March 2014	Refer CGICTPF	3	Nil	Head of Department	GITO
2	Limpopo department of education CGICT Policy framework	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	2	Nil	Head of Department	Designated Governance Champion
3	Limpopo department of education CGICT Charter	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	2	Nil	Head of Department	Designated Governance Champion, GITO
4	Governance and Management of ICT Framework	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	2	Nil	Head of Department	Designated Governance Champion, GITO
5	Risk Management Policy with relation to ICT	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	2	Nil	Head of Department of Provincial Treasury	Chief Audit Executive
6	Internal Audit plan that includes ICT	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	2	Nil	Head of Department of Provincial Treasury	Chief Audit Executive
7	ICT Portfolio Management Framework	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	2	Nil	Head of Department	GITO
8	ICT Security Policy	March	Refer paragraph 9.2.4.2 Corporate	3	Nil	Head of Department	GITO

#	Initiative	Due Date	Comments	Duration in months	Estimated cost	RACI	
		2014	Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.				
9	Business Continuity Plan (BCP)	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	4	Nil	Head of Department	Senior General manager ; Corporate Services
10	ICT Continuity Policy and Plan	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	4	Nil	Head of Department	GITO
11	Change management Plan for the implementation of CGICT and GICT	March 2014	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	2	Nil	Head of Department	GITO
12	Enterprise Architecture	March 2015	Refer paragraph 9.2.4.2 Corporate Governance of ICT Policy Framework Compulsory Programs for a mapping to the COBIT 5 IT Processes.	9	Nil	Head of Department	Senior General manager Education Planning and Quality Assurance/ Enterprise Architect, GITO
COBIT 4.1							
16	PO2 Define the Information Architecture	March 2015	Will form part of the Enterprise Architecture project as per the number 15 initiative.		Nil	Head of Department	GITO
17	PO3 Determine Technological Direction	March 2015	Will form part of the Enterprise Architecture project as per the number 15 initiative		Nil	Head of Department	GITO
18	PO4 Define the IT Processes, Organisation and Relationships	After March 2014	To be incorporated into the number 4 initiative		Nil	Head of Department	GITO
19	PO8 Manage Quality	After March 2014		3	Nil	Head of Department	GITO
20	PO9 Assess and Manage IT Risks	March 2014	To be incorporated into the number 5 initiative		Nil	Head of Department	GITO
21	PO10 Manage Projects	March 2014	To be incorporated into the number 7 initiative		Nil	Head of Department	GITO
22	AI2 Acquire and Maintain Application Software	After March 2014		3	Nil	Nil	Nil
23	AI6 Manage Changes	After		3	Nil	Nil	Nil

#	Initiative	Due Date	Comments	Duration in months	Estimated cost	RACI	
		March 2014					
24	AI7 Install and Accredit Solutions and Changes	After March 2014		3	Nil	Nil	Nil
25	DS4 Ensure Continuous Service	March 2014	To be incorporated into the number 10 initiative		Nil	Nil	Nil
26	DS8 Manage Service Desk and Incidents	After March 2014		3	Nil	Nil	Nil
27	DS9 Manage the Configuration	After March 2014		3	Nil	Nil	Nil
28	DS10 Manage Problems	After March 2014		3	Nil	Nil	Nil
Total					Nil		

The table below depicts the IT process accountability and Responsibilities.

Legend:

R = Responsible	Refers to the person who must **ensure** that **activities are completed successfully.**
A = Accountable	Refers to the person or group who has the authority to **approve or accept** the execution of an activity.

Note:
The costing for IT Governance initiatives from the IT Governance Capability Maturity assessments is for the development of frameworks, policies, processes and procedures. The costing for IT Process automation tools has been excluded.

The cost for executing an ICT Strategic Plan (GWEA) is based on quotations delivered by SITA to the department. The costing for the acquisition of a CASE tool has been excluded.

The estimated costs are based on an out-sourcing model. Some of these deliverables already exists and the cost for these deliverables would therefore be nil.

12 Conclusion and way forward

12.1 IT Governance COBIT 4.1 Improvement initiatives

This report gives a relative measure of where the department finds itself currently in terms of IT governance maturity and how to improve these maturity levels.

The initiatives contained herein should be executed according to proper project management principles. The initiatives contained herein should be translated into an activity schedule, project team members assigned and resources such as funding set aside.

A department should decide on the sourcing option going forward, e.g. executing these projects internally, co-sourcing or outsourcing. In all instances the project team members should have the necessary knowledge to implement the initiatives.

Consideration should be given to adopting other best practices such as ITIL and ISO9001, over and above COBIT when implementing initiatives. Refer Annex C: Limpopo department of education ICT Framework-, Processes-, Plans-, Procedures- and Policies Framework, for more information.

It is recommended that all COBIT 4.1 initiatives that do not support the CGICTPF be deferred until after March 2014, in order to give priority to the CGICTPF initiatives.

12.2 CGICTPF Compulsory Programs

Immediate action should be taken to start the deliverables due by March 2014. The department has adopted the CGICTPF principles, practices and objectives, as depicted in Annex B: ICT Governance Principles, Practices and Objectives.

Furthermore it is recommended that the department:

a) Extend the CGICTPF program deliverables to process level (e.g. The ICT Portfolio Management Framework is only a portion of ICT process APO05: Manage portfolio)
b) Position themselves to achieve all Process Outcomes (level 1) for the related CGICTPF processes
c) Develop and implement all Work Products (level 2) for the related CGICTPF processes
    - Requirements for the work products of the process are defined.
    - Requirements for documentation and control of the work products are defined.
    - Work products are appropriately identified, documented, and controlled.
    - Work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.
d) Achieve process attributes fully (level 2) for the related CGICTPF processes
    - Objectives for the performance of the process are identified.
    - Performance of the process is planned and monitored.
    - Performance of the process is adjusted to meet plans.
    - Responsibilities and authorities for performing the process are defined, assigned and communicated.

- Resources and information necessary for performing the process are identified, made available, allocated and used.
- Interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility.

Annex A: Definitions

Accountable	A person or group who has the authority to approve or accept the execution of an activity
Balanced scorecard	A coherent set of performance measures organised into four categories. It includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives. It was developed by Robert S. Kaplan and David P. Norton in 1992.
Control objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process
Control practice	Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business
Data classification scheme	An enterprise-wide scheme for classifying data by factors such as criticality, sensitivity and ownership
Data dictionary	A database that contains the name, type, range of values, source and authorisation for access for each data element in a database. It also indicates which application programs use that data so that when a data structure is contemplated, a list of the affected programs can be generated. The data dictionary may be a stand-alone information system used for management or documentation purposes, or it may control the operation of a database.
Enterprise governance	"A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly," IT Governance Institute
Information Technology tactical plan	A medium-term plan, i.e., six- to 18-month horizon, that translates the IT strategic plan direction into required initiatives, resource requirements, and ways in which resources and benefits will be monitored and managed
Information Technology	Information technology; the hardware, software, communications and other facilities used to input, store, process, transmit and output data in whatever form
Maturity	In business, indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives
Measure	A standard used to evaluate and communicate performance against expected results Scope Note: Measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction. Reporting and monitoring measures help an enterprise gauge progress toward effective implementation of strategy.
Metrics	A quantifiable entity that allows the measurement of the achievement of a process goal. Scope Note: Metrics should be SMART--specific, measurable, actionable, relevant and timely. Complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate) and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment.
Operational Level Agreement	Operational level agreement; an internal agreement covering the delivery of services that support the IT organisation in its delivery of services
Organisation	The manner in which an enterprise is structured; can also mean the entity
Policy	1. Generally, a document that records a high-level principle or course of action that has been decided on The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. Scope Note: In addition to policy content, policies need to describe the consequences of

	failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured. 2. Overall intention and direction as formally expressed by management.
Portfolio	A grouping of programmes, projects, services or assets selected, managed and monitored to optimise business return
Procedure	A document containing steps that specify how to achieve an activity. Procedures are defined as part of processes.
Process	Generally, a collection of procedures influenced by the organisation's policies and procedures that takes inputs from a number of sources, including other processes, manipulates the inputs, and produces outputs, including other processes. Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.
Responsible	A person who must ensure that activities are completed successfully
Risk	In business, the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets; usually measured by a combination of impact and probability of occurrence
Root cause analysis	Process of diagnosis to establish origins of events, which can be used for learning from consequences, typically of errors and problems
Service desk	A point of contact within the IT organisation for users of IT services
Service provider	External entity that provides services to the organisation
Service Level Agreement	Service level agreement; an agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured

Overview of COBIT 4.1 Domains and IT Processes

The following table contains a brief overview of each of the COBIT® domains.

Table 19: Brief overview of the COBIT® domains

Domain	Brief overview
PO: Plan and Organise	Addresses strategy and tactics, and concerns identifying the way IT can best contribute to achieving the business objectives. The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organisation as well as technological infrastructure should be put in place.
AI: Acquire and Implement	Realises the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are addressed by this domain to ensure the solutions continue meeting the business objectives.
DS: Deliver and Support	Concerned with the actual delivery of required services, including service delivery, managing security and continuity, service support for users, and managing data and operational facilities.
ME: Monitor and Evaluate	Concerned with assessing all IT processes on a 'need to be regularly assessed' over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring internal control, regulatory compliance and governance.

The following table provides a brief overview of each of the IT processes, the detailed descriptions are included in each domain hereunder.

Table 20: Brief overview of the COBIT® IT processes

IT Process	Brief overview
PO1 Define a strategic ICT plan	IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities.
PO2 Define the information architecture	The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information.
PO3 Determine the technological direction	The information services function determines the technology direction to support the business.
PO4 Define the IT processes, organisation and relationships	An IT organisation is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision.
PO5 Manage the ICT investment	A framework is established and maintained to manage IT-enabled investment programmes and that encompasses cost, benefits, prioritisation within budget, a formal budgeting process and management against the budget.
PO6 Communicate management aims and direction	Management develops an enterprise IT control framework and defines and communicates policies.
PO7 Manage IT HR	A competent workforce is acquired and maintained for creating and delivering IT services to the business.

IT Process	Brief overview
PO8 Manage quality	A QMS is developed and maintained that includes proven development and acquisition processes and standards.
PO9 Assess and manage IT risks	A risk management framework is created and maintained.
PO10 Manage projects	A programme and project management framework for managing all IT projects is established.
AI1 Identify automated solutions	The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach.
AI2 Acquire and maintain application SW	Applications are made available in line with business requirements.
AI3 Acquire and maintain technology infrastructure	Organisations have processes for acquiring, implementing and upgrading the technology infrastructure.
AI4 Enable operation and use	Knowledge about new systems is made available.
AI5 Procure IT resources	IT resources, including people, HW, SW and services, need to be procured.
AI6 Manage changes	All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner.
AI7 Install and accredit solutions and changes	New systems need to be made operational once development is complete.
DS1 Define and manage service levels	Effective communication between IT management and business customers regarding services required is enabled by a documented definition of an agreement on IT services and service levels.
DS2 Manage third party services	The need to ensure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third party management process.
DS3 Manage performance and capacity	The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources.
DS4 Ensure continuous service	The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, using offsite backup storage and providing periodic continuity plan training.
DS5 Ensure systems security	The need to maintain the integrity of information and protect IT assets requires a security management process.
DS6 Identify and attribute costs	The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation.
DS7 Educate and train users	Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group.
DS8 Manage service desk and incidents	Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process.
DS9 Manage the configuration	Ensuring the integrity of HW and SW configurations requires establishing and maintaining an accurate and complete configuration repository.

IT Process	Brief overview
DS10 Manage problems and incidents	Effective problem management requires identifying and classifying problems, root cause analysis and resolving problems.
DS11 Manage data	Effective data management requires identifying data requirements.
DS12 Manage the physical environment	Protection for computer equipment and personnel requires well-designed and well-managed physical facilities.
DS13 Manage operations	Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of HW.
ME1 Monitor and evaluate IT performance	Effective IT performance management requires a monitoring process.
ME2 Monitor and evaluate internal control	Establishing an effective internal control programme for IT requires a well-defined monitoring process.
ME3 Ensure compliance with external requirements	Effective oversight of compliance requires establishing a review process to ensure compliance with laws, regulations and contractual requirements.
ME4 Provide IT governance	Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered according to enterprise strategies and objectives.

Annex B: ICT Governance Principles, Practices and Objectives

B.1. ICT Principles

Governance Principles are required to act as the vehicle to translate the desired behaviour into practical guidance for day-to-day management (Source: Limpopo department of education Corporate Governance of Information and Communication Technology Policy Framework (CGICTPF).

a. **Principle 1: Political Mandate**
   The Corporate Governance of ICT must enable the department's political mandate.
   The Executive Authority must ensure that Corporate Governance of ICT achieves the political mandate of the department.
b. **Principle 2: Strategic Mandate**
   The Corporate Governance of ICT must enable the department's strategic mandate.
   The HoD must ensure that Corporate Governance of ICT achieves the department's strategic plans.
c. **Principle 3: Corporate Governance of ICT**
   The HoD is responsible for the Corporate Governance of ICT. The HoD must create an enabling environment in respect of the Corporate Governance of ICT within the applicable legislative and regulatory landscape and information security context.
d. **Principle 4: ICT Strategic Alignment**
   ICT service delivery must be aligned with the strategic goals of the department. Executive Management must ensure that ICT service delivery is aligned with the departmental strategic goals and that business accounts for current and future capabilities of ICT. It must ensure that ICT is fit for purpose at the correct service levels and quality for both current and future business needs.
e. **Principle 5: Significant ICT Expenditure**
   Executive Management must monitor and evaluate significant ICT expenditure. Executive Management must monitor and evaluate major ICT expenditure, ensure that ICT expenditure is made for valid business enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed.
f. **Principle 6: Risk Management and Assurance**
   Executive Management must ensure that ICT risks are managed and that the ICT function is audited. Executive Management must ensure that ICT risks are managed within the departmental risk management practice. It must also ensure that the ICT function is audited as part of the departmental audit plan.
g. **Principle 7: Organisational Behaviour**
   Executive Management must ensure that ICT service delivery is sensitive to organisational behaviour/culture. Executive Management must ensure that the use of ICT demonstrates the understanding of and respect for organisational behaviour/culture

B.2. ICT Practices

The table below contains the ICT Practices as prescribed by the CGICTPF.

Table 21: ICT Practices

Practice number	Practice Description
1	**The Executive Authority must:** (a) provide political leadership and strategic direction, determine policy and provide oversight;

Practice number	Practice Description
	(b) ensure that ICT service delivery enables the attainment of the strategic plan; (c) take an interest in the Corporate Governance of ICT to the extent necessary to ensure that a properly established and functioning Corporate Governance of ICT system is in place in the department to leverage ICT as a business enabler; (d) assist the HoD to deal with intergovernmental, political and other ICT related business issues beyond their direct control and influence; and (e) ensure that the department's organisational structure makes provision for the Corporate Governance of ICT.
2	**Vertical Sector Mandate** The Executive Authority of national departments that have a sector / functional area specific responsibility or sphere of influence must ensure that the necessary cross sector/functional area Corporate Governance of ICT arrangements are in place.
3	**The Head of Department must:** (a) provide strategic leadership and management; (b) ensure alignment of the ICT strategic plan with the departmental and business strategic plans; (c) ensure that the Corporate Governance of ICT is placed on the department's strategic agenda; (d) ensure that the Corporate Governance of ICT Policy Framework, charter and related policies for the institutionalisation of the Corporate Governance of ICT are developed and implemented by Executive Management; (e) determine the delegation of authority, personal responsibility and accountability to the Executive Management with regards to the Corporate Governance of ICT; (f) ensure the realisation of department-wide value through ICT service delivery and management of business and ICT related risks; (g) ensure that appropriate Corporate Governance of and Governance of ICT capability and capacity are provided and a suitably qualified and experienced Governance Champion is designated , who must function at Executive Management level (h) Ensure that appropriate ICT capacity and capability are provided and a suitably qualified and experienced GITO, who must function at Executive Management level, is appointed ; and (i) Ensure the monitoring and evaluation of the effectiveness of the Corporate Governance of ICT system.
4	**A Risk and Audit Committee must assist the HoD** in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.
5	**EMC (Executive Management Committee) must ensure:** (a) ICT strategic goals are aligned with the department's business strategic goals and support strategic business processes; and (b) Business related ICT strategic goals are cascaded throughout the department for implementation and are reported on. (c) Means and Mechanisms: (i) Advice is provided to the HoD regarding all aspects of the Corporate Governance of and Governance of ICT; (ii) The Corporate Governance of and Governance of ICT is implemented and managed; (iii) The necessary strategies, architectures, plans, frameworks, policies, structures (including outsourcing), procedures, processes, mechanisms and controls, and culture regarding all aspects of

Practice number	Practice Description
	ICT use (business and ICT) are clearly defined, implemented, enforced and assured through independent audits; (iv) The responsibility for the implementation of the Corporate Governance of and Governance of ICT is delegated and communicated to the relevant management (senior business and ICT management); (v) Everyone in the department understands the link between business and ICT strategic goals and accepts their responsibilities with respect to the supply and demand for ICT; (vi) Significant ICT expenditure is informed by the department's Service Delivery Plan, Enterprise Architecture and ICT Architecture, motivated by business cases, monitored and evaluated; (vii) The planning and execution of ICT adheres to relevant judicial requirements; and (viii) ICT related risks are managed. (d) ICT Security: (i) An information security strategy is approved; (ii) Intellectual property in information systems is appropriately protected; and (iii) ICT assets, privacy, security and the personal information of employees are effectively managed. (e) Organisational Behaviour/Culture: The use of ICT demonstrates the understanding of and respect for organisational behaviour/culture, which should include human behaviour

B.3. OBJECTIVES OF THE CORPORATE GOVERNANCE OF ICT

In order to give effect to the Corporate Governance of ICT in the Public Service, the following objectives were adopted by the GITOC:

a. Identify, establish and prescribe a uniform Governance of ICT Framework (GICTF) and implementation guideline for the Public Service,
b. Embed the Corporate Governance of and Governance of ICT as a subset of Corporate Governance,
c. Create business value through ICT enablement by ensuring business and ICT strategic alignment,
d. Provide relevant ICT resources, organisational structure, capacity and capability to enable ICT service delivery,
e. Achieve and monitor ICT service delivery performance and conformance to relevant internal and external policies, frameworks, laws, regulations, standards and practices;
f. Implement the governance of ICT in the department, based on the COBIT process framework, and
g. Position the GITO function as an integral part of Executive Management.

Annex C: Limpopo department of education ICT Framework-, Processes-, Plans-, Procedures- and Policies Framework

The table below depicts the relevant IT Process and Control Objective with accompanying source, frameworks, processes, plans, procedure and policies.

This represents the target IT Governance framework for the department.

Table 22: ICT Frameworks, Processes, Plans, Procedures and Policies Frameworks

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
PO2 Define the Information Architecture **COBIT 5:** ▪ **APO01 Manage the IT Management Framework** ▪ **APO03 Manage Enterprise Architecture**	PO2.1	APO03.02	NA	NA	NA	NA	NA
	PO2.2	APO03.02	NA	NA	NA	NA	NA
	PO2.3	APO03.02	NA	NA	NA	NA	NA
	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
PO3 Determine Technological Direction **COBIT 5:** ▪ **APO01 Manage the IT Management**	PO3.1	APO02.03; APO04.03				Technology plan.	
	PO3.2	APO02.03; APO02.04; APO02.05; APO04.03; APO04.04; APO04.05				Technology Infrastructure Plan	

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
Framework ▪ **APO02 Manage Strategy** ▪ **APO03 Manage Enterprise Architecture** ▪ **APO04 Ensure Governance Framework Setting and Maintenance**	PO3.3	EDM01.01; APO04.03		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		A process to prevent the acquisition of non-conforming systems or applications. Put in place monitoring and benchmarking processes, such as measuring non-compliance to technology standards, to ensure compliance to the standards.			
	PO3.5	APO01.01		A process to monitor and benchmark the effect on business strategy and identify instances of non-compliance to technology standards.			
PO4 Define the IT Processes, Organisation and Relationships **COBIT 5:** ▪ **APO01: Manage the IT Management**	PO4.1	APO01.03; APO01.07	A framework to enable the definition and follow-up of process goals, measures, controls and maturity.			IT process framework	
	PO4.2	APO01.01	NA	NA	NA	NA	NA
	PO4.3	APO01.01	NA	NA	NA	NA	NA
	PO4.4	APO01.05	NA	NA	NA	NA	NA

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
Framework ▪ **APO07: Manage Human Resources** ▪ **APO11: Manage Quality**	PO4.5	APO01.01		A process for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances			
	PO4.6	APO01.02	NA	NA	NA	NA	NA
	PO4.7	APO11.01	NA	NA	NA	NA	NA
	PO4.9	APO01.06			Policies to ensure appropriate and consistent enterprise-wide classification of data.		Data and System Ownership procedures
	PO4.10	APO01.02		A process for escalating issues that are identified through supervisory processes.			
	PO4.11	APO01.02	NA	NA	NA	NA	NA
	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.
	PO4.14	APO07.06			Contracted Staff Policies and Procedures		
	PO4.15	APO01.01	NA	NA	NA	NA	NA
PO8 Manage Quality **COBIT 5:** ▪ **APO11: Manage**	PO8.1	APO11.01				Project quality plans	
	PO8.2	APO11.02					IT Standards and Quality Practices procedures

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
Quality	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 development		Procedures, as part of the development and acquisition standards, that provide appropriate and 'fit for purpose' guidelines for controlled development
	PO8.4	APO11.03					
	PO8.5	APO11.06				A quality plan that promotes continuous improvement.	
	PO8.6	APO11.04	NA	NA	NA	NA	NA
PO9 Assess and Manage IT Risks **COBIT 5:** ▪ **EDM03: Ensure Risk Optimisation** ▪ **APO01: Manage the IT Management Framework** ▪ **APO12: Manage Risk**	PO9.1	EDM03.02; APO01.03	An IT risk management framework aligned to the organisation's (enterprise's) risk management framework				
	PO9.2	APO12.03	NA	NA	NA	NA	NA
	PO9.3	APO12.01; APO12.03	NA	NA	NA	NA	NA
	PO9.4	APO12.02; APO12.04	NA	NA	NA	NA	NA
	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		A risk action plan	

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
				levels			
	PO9.6	APO12.04; APO12.05	NA	NA	NA	NA	NA
PO10 Manage Project **COBIT 5:** ▪ **BAI01: Manage Programmes and Projects**	PO10.1	BAI01.01	NA	NA	NA	NA	NA
	PO10.2	BAI01.01	A project management framework that defines the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. Ensure that the framework and supporting method are integrated with the programme management processes	A change control process for recording, evaluating, communicating and authorising changes to the project scope, project requirements or system design			
	PO10.3	BAI01.01	NA	NA	NA	NA	NA
	PO10.4	BAI01.03	NA	NA	NA	NA	NA
	PO10.5	BAI01.07				A project communication plan that identifies internal and external project communications.	
	PO10.6	BAI01.07	NA	NA	NA	NA	NA
	PO10.7	BAI01.08				Integrated Project	

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
						Plans	
	PO10.8	BAI01.08	NA	NA	NA	NA	NA
	PO10.9	BAI01.10	A project risk management framework that includes identifying, analysing, responding to, mitigating, monitoring and controlling risks.				
	PO10.10	BAI01.09				Project Quality Plan	
	PO10.11	BAI01.11	NA	NA	NA	NA	NA
	PO10.12	BAI01.08	NA	NA	NA	NA	NA
	PO10.13	BAI01.06; BAI01.11	NA	NA	NA	NA	NA
	PO10.14	BAI01.13	NA	NA	NA	NA	NA
AI2 Acquire and Maintain Application Software **COBIT 5:** ▪ **BAI03: Manage Solutions Identification and Build**	AI2.1	BAI03.01	NA	NA	NA	NA	NA
	AI2.2	BAI03.02	NA	NA	NA	NA	NA
	AI2.3	BAI03.05	NA	NA	NA	NA	NA
	AI2.4	BAI03.01; BAI03.02; BAI03.03; BAI03.05	NA	NA	NA	NA	NA
	AI2.5	BAI03.03; BAI03.05	NA	NA	NA	NA	NA
	AI2.6	BAI03.10	NA	NA	NA	NA	NA
	AI2.7	BAI03.03; BAI03.04					Development procedures
	AI2.8	BAI03.06				Software QA plans	
	AI2.9	BAI03.09		A process for standardising, tracking, recording and approving all change requests during development of application systems.			

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	**Processes**	**Policies**	**Plans**	**Procedures**
	AI2.10	BAI03.10		A process for application software maintenance activities.		A plan for the maintenance of software applications.	
AI6 Manage Changes **COBIT 5:** ▪ **BAI06: Manage Changes**	AI6.1	BAI06.01; BAI06.02; BAI06.03; BAI06.04	A change management framework that specifies the policies and processes, including: • Roles and responsibilities • Classification and prioritisation of all changes based on business risk • Assessment of impact • Authorisation and approval of all changes by the business process owners and IT • Tracking and status of changes • Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention)				Change management procedures for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.
	AI6.2	BAI06.01		A process to allow business process owners and IT to request changes to infrastructure, systems or applications.			

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
	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.			
	AI6.5	BAI06.04	NA	NA	NA	NA	NA
AI7 Install and Accredit Solutions and Changes **COBIT 5:** ▪ **BAI05: Manage Organisational Change Enablement** ▪ **BAI07: Manage Change Acceptance and Transitioning**	AI7.1	BAI05.05				Training and implementation plan	
	AI7.1	BAI05.05				A plan for planned changes	
	AI7.2	BAI07.01; BAI07.03				Test Plan	
	AI7.3	BAI07.01				Implementation and fall-back/back out plans	
	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. Consider the effect of regulatory			

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	**Processes**	**Policies**	**Plans**	**Procedures**
				or compliance requirements			
	AI7.5	BAI07.02	NA	NA	NA	NA	NA
	AI7.6	BAI07.05	NA	NA	NA	NA	NA
	AI7.7	BAI07.05	NA	NA	NA	NA	NA
	AI7.8	BAI07.06		An approval process for application, system and configuration transfer from testing to the production environment exists.			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				Action plan to address issues identified in the post-implementation review.	Post-implementation procedures
	AI7.9	BAI07.08					Procedures for post-implementation reviews
DS4 Ensure Continuous Service **COBIT 5:** ▪ **DSS04 Manage Continuity**	DS4.1	DSS04.01;DSS04.02	A framework for IT continuity to support enterprise-wide business continuity management using a consistent process.		Policies for conducting regular tests		Documentation standards and change management procedures for all IT continuity-related procedures and tests

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
	DS4.2	DSS04.03				IT Continuity Plans	Emergency procedures to ensure the safety of all affected parties, including coverage of occupational health and safety requirements
	DS4.3	DSS04.04	NA	NA	NA	NA	NA
	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.
	DS4.5	DSS04.05	NA	NA	NA	NA	NA
	DS4.6	DSS04.07	NA	NA	NA	NA	NA
	DS4.7	DSS04.03		A distribution process that: • Distributes the IT continuity plan in a timely manner to all recipients and locations on the distribution list • Collects and destroys obsolete copies of the plan in line with the organisation's policy for discarding confidential information			Procedures documenting instructions for storage of confidential information.
	DS4.8	DSS04.04					Resumption procedures.
	DS4.9	DSS04.08	NA	NA	NA	NA	NA
	DS4.10	DSS04.09					Procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
							disaster
	DS8.2	DSS02.01; DSS02.02;DSS02.03	NA	NA	NA	NA	NA
	DS8.3	DSS02.04		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			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;DSS02.06		A process to manage the resolution and closure of each incident, including use of predetermined categorisations to identify the likely root cause of the incident.			Procedures for the monitoring of timely clearance of customer queries.
	DS8.5	DSS02.07		Define a process to identify, investigate and report on all queries in which the agreed-upon time frames for resolution (e.g., SLAs) were exceeded.			

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	**Processes**	**Policies**	**Plans**	**Procedures**
DS9 Manage the Configuration **COBIT 5:** ▪ **BAI10: Manage Configuration** ▪ **DSS02: manage Service Requests and Incidents**	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 process to record new, modified and deleted Configuration items and their relative attributes and versions. A process to maintain an audit trail for all changes to configuration items. A process to identify critical configuration items in relationship to business functions (component failure impact analysis). Define and implement a process to ensure that valid licences are in place to prevent the inclusion of unauthorised software	A policy that integrates incident, change and problem management procedures with the maintenance of the configuration repository.		C**onfiguration procedures** to support management and logging of all changes to the configuration repository
	DS9.3	BAI10.04; BAI10.05; DSS02.05		Implement 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 Manage Problems **COBIT 5:** ▪ **DSS03: Manage**	DS10.1	DSS03.01		A process to report and classify problems that have been identified as part of incident management.			

IT Process	Control Objective	COBIT 5 Process Reference	COBIT 4.1				
			Frameworks	Processes	Policies	Plans	Procedures
Problems	DS10.1	DSS03.01		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).			
	DS10.2	DSS03.02					Problem management procedures for the tracking of problem trends.
	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.			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.
	DS10.4	DSS03.05		A process to capture problem information related to IT changes and to communicate it to key stakeholders. A process to capture change efforts resulting from problem management process activities (e.g., fixes to problems and known errors) and report on them.			

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

The following Standards, Legislation, Best practises should be considered when developing IT Processes.

Table 23: Standards, Legislation, Best practises per IT domain

Domain	Standards, Legislation, Best practises
PO	SANS9001: Quality management systems — Requirements
AI	a. PFMA b. SITA Act c. SDLC e.g. Rational Unified Process (RUP) d. MISS e. MIOS f. SANS16326: Systems and software engineering - Life cycle processes - Project management
DS	a. CGICTF b. ITIL c. SANS20000-1: Information technology - Service management Part 1: Service management system requirements d. SANS20000-3: Information technology - Service management Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1 e. SANS20000-2: Information technology - Service management Part 2: Code of practice f. SANS20000-5: Information technology - Service management Part 5: Exemplar implementation plan for ISO/IEC 20000-1 g. SANS12207: Systems and software engineering - Software life cycle processes h. SANS 22301:2012 Societal security - Business continuity management systems - Requirements i. SANS27000: Information technology - Security techniques - Information security management Systems - Overview and vocabulary j. SANS21827: Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®)
ME	a. MPAT

Annex D: Rating Scales

The table below depicts the Performance rating scales that were used during the assessments.

Table 24: Performance assessment levels

Level	Performance	Description
5	**Everything is always done well**	• Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. • IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.
4	**Parts are always done well**	• Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. • Automation and tools are used in a limited or fragmented way.
3	**All aspects sometimes**	• Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
2	**Some aspects sometimes**	• 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.
1	**Some aspects rarely**	• 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 table below depicts the Importance rating scales that were used during the assessments.

Table 25: Importance Assessment Levels

Level	Performance
5	Critical
4	Very significant
3	Make things easier
2	Can survive without it if necessary
1	Not at all

Annex E: Acronyms

AI	acquire and implement
BAS	basic accounting system
BIA	business impact analysis
CFO	chief financial officer
CISA	certified information systems auditor
CMDB	configuration management database
CO	control objective
COBIT©	Control Objectives for Information and related Technology
CTO	Chief Technology Officer
DRP	disaster recovery plan
DS	deliver and support
DVD	digital versatile disk
EAP	employee assistance program
EXCO	executive committee
GITO	government information technology officer
GM	General Manager
GWEA	Government Wide Enterprise Architecture
HIV	human immune deficiency virus
HR	Human Resources
HRD	Human Resources Development
HRM	Human Resources Manager
HW	hardware
ICT	Information and Communication Technology
IFMS	integrated financial management system
IPS	intelligent protection switching
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organisation
IT	Information Technology
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
Department	Limpopo department of education
ME	monitor and evaluate
MIOS	minimum interoperability standards
MISS	minimum information security standard
MS	Microsoft
OD	organisational development
OLA	operational level agreement
PFMA	Public Finance Management Act
PMBOK	project management body of knowledge
PMS	Performance Management System
PO	plan and organise
PRINCE2	PRINCE2 is a project management methodology
QA	quality assurance
QMS	quality management system
RFC	request for change
ROI	return on investment
ROM	read only memory
SANS	South African National Standards
SCM	software configuration management
SDLC	systems development life cycle
SITA	State Information Technology Agency
SLA	service level agreement
SW	software
SWOT	strengths, weaknesses, opportunities and threats