IT Governance Framework and Implementation Roadmap

This document is confidential.

Date	: March 2016
Document name	: uMfolozi Local Municipality IT Governance Framework and Implementation Roadmap
Document version	: Final

Document Control

Document **Information**

	Information
Document Id	
Document Owner	
Issue Date	

Document **History**

Version	Issue Date	Changes
[1.0]	*[Date]*	*[Section, Page(s) and Text Revised]*
	01/03/2016	Review

Table of Contents

1. Introduction

A need for a well governed IT function is becoming more apparent as business leaders are forced to critically evaluate their cost and value chains in challenging economic environments. Additionally, their compliance, audit, risk and security environments are becoming the focus of attention in a world where regulatory compliance can fundamentally impair or enable the operations of a company, whether in the private sector or in government.

2.   Executive Summary

A need for a well governed IT function is becoming more apparent as business leaders are forced to critically evaluate their cost and value chains in challenging economic environments. Globally, enterprises—whether public or private, large or small—increasingly understand that information is a key resource and that IT is a strategic asset and important contributor to success. Additionally, their compliance, audit, risk and security environments are becoming the focus of attention in a world where regulatory compliance can fundamentally impair or enable the operations of a business.

uMfolozi Local Municipality, with the assistance of AdvisoryIT, have formed a customised IT Governance Framework and implementation roadmap focussing on the governance of the IT function across uMfolozi . This governance framework is broken into major components, namely the IT goals based on business priorities, the prioritised IT Governance Framework, the IT Governance implementation roadmap and the IT Governance task list.

The IT Governance Framework takes into account both the risk mitigation and performance considerations required to create a complete IT governance overview. The COBIT framework has been utilised to provide the basis for the IT Governance Framework. COBIT focuses on implementing governance within IT, controlling IT and monitoring the performance of IT. An understanding of the uMfolozi stakeholder needs was sort followed by an assessment based on the Kaplan-Norton Balanced Scorecard to determine the key priorities of the municipality. These were then used to extract the associated key IT goals, used to define the required performance elements of the IT Governance Framework. Finally, an implementation roadmap for the governance framework was formulated based on the input from the IT Strategy development Architecture workshops and risk and performance workshops with the IT Manager. This approach ensures that this IT Governance Framework and implementation roadmap has been formed to include the relevant areas for uMfolozi from the industry accepted IT governance agendas.

Numerous supporting sheets are provided to interpret the IT Governance Framework which includes Business and IT priorities, role definitions, governance implementation task lists, proposed implementation timelines and dependencies, as well as guidance on how the framework and roadmap is to be used.

3. Background to IT Governance

A need for a well governed IT function is becoming more apparent as business leaders are forced to critically evaluate their cost and value chains in challenging economic environments. Globally, enterprises—whether public or private, large or small—increasingly understand that information is a key resource and that IT is a strategic asset and important contributor to success. Additionally, their compliance, audit, risk and security environments are becoming the focus of attention in a world where regulatory compliance can fundamentally impair or enable the operations of a business.

Governance of Enterprise IT ("GEIT") is a subset discipline of Corporate Governance focused on Information Technology as a resource and their risk and performance management. The rising interest in IT Governance is partly due to compliance initiatives, for instance Sarbanes-Oxley in the USA, Basel II in Europe and King III in South Africa, as well as the acknowledgement that IT investments can easily get out of control and profoundly affect the performance of an organisation.

Successful enterprises have recognised that the board and executives need to embrace IT like any other significant part of doing business. Boards and management—both in the business and IT functions—must collaborate and work together, so that IT is included within the governance and management approach. The traditional involvement of board-level executives in IT issues was to defer all key decisions to the company's IT professionals. IT Governance implies a system in which all stakeholders, including the board, internal customers, and in particular departments such as finance, have the necessary input into the decision making process. This prevents IT from independently making and later being held solely responsible for poor decisions. It also prevents critical users from later finding that the system does not behave or perform as expected.

The discipline of GEIT is supported by a number of reference frameworks to guide its implementation. Of these probably the most prominent are Control Objectives for Information and related Technology ("COBIT"), the IT Infrastructure Library ("ITIL")

and ISO27001 (previously ISO17799). GEIT, like Corporate Governance, is a framework that is implemented to support a business. Since no two businesses are exactly alike, it stands to reason that their governance frameworks would need to be catered to the specific resource, risk and performance environment that they operate in. As such, reference frameworks should not be taken as verbatim implementation templates for an organisation, but rather as starting points for a guided discussion on the best governance framework for the organisation.

4. Approach

The IT Governance Framework helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. The COBIT framework (version 5.0) has been utilised to provide the basis for the IT Governance Framework. COBIT 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. The outcome of the Enterprise Architecture workshops performed as part of the IT Strategy development was used as input to understand the municipality's value chain and priorities.

An understanding of the uMfolozi stakeholder needs was followed by an assessment based on the Kaplan-Norton Balanced Scorecard to determine the key priorities of the municipality. These were then used to extract the associated key IT goals, used to define the required performance elements (enablers) of the IT Governance Framework. Finally, an implementation roadmap for the governance framework was formulated based on the risk and performance workshops with the IT Manager. This approach ensured that this IT Governance Framework and implementation roadmap has been formed to include the relevant areas for uMfolozi from the industry accepted IT Governance agendas.

The diagram below depicts the general process followed in order to arrive at the IT Governance Framework and implementation roadmap: Below is an itemised breakdown of the steps taken to form the IT Governance Framework, roadmap and priority 1 task list.
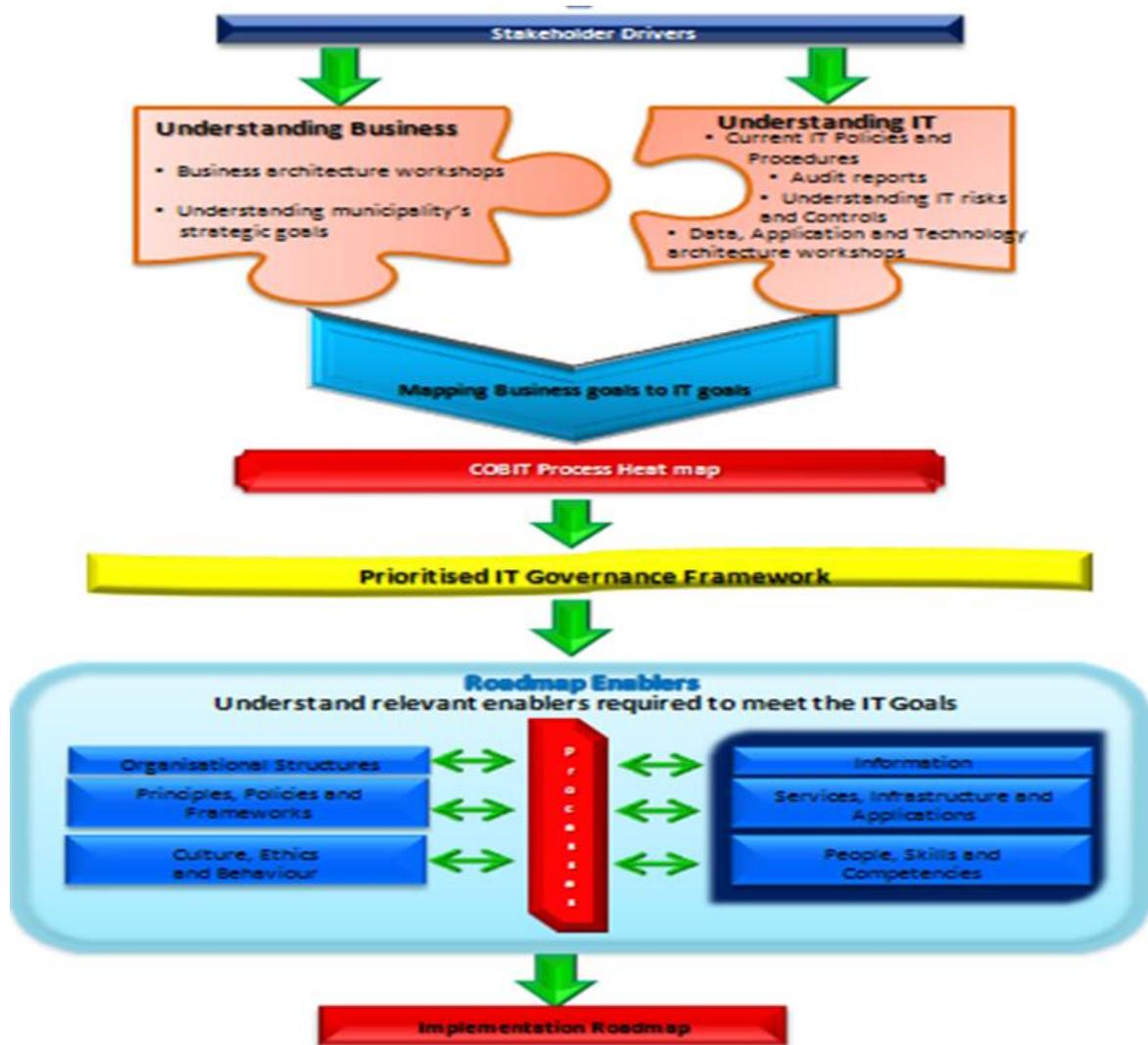

1. A stakeholder-driver understanding workshop was performed with the Performance manager responsible for the IDP and its execution and the IT manager to confirm the stakeholder values from interpretation of the IDP.
2. A review of the results of the Architecture workshops performed as part of the development of an IT Strategy was performed to understand the business priorities for uMfolozi

3. A review of the risk register and IT audit reports and discussions with the IT manager was performed to understand the risks and controls faced by uMfolozi

4. A business priority workshop was performed with the Performance manager responsible for the IDP and its execution and the IT manager to confirm key business goals of uMfolozi from interpretation of the IDP, based on the Kaplan-Norton Balanced Scorecard.

5. The key municipality goals were linked to their related IT goals. These IT goals were then matched to their required COBIT enablers.

6. A COBIT process "heat map" was formed based on IT goals, supplemented with areas identified from analysing the IDPs, IT audit reports, risk register, uMfolozi Architecture documentation and general good practice. This heat map was used to identify the priority 1, 2 and 3 IT Governance areas for the municipality

7. A workshop was held with IT to identify key documents and the related task list for priority 1 areas

5. COBIT 5 Overview

Information is a key resource for all enterprises, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Successful enterprises have recognised that the board and executives need to embrace IT like any other significant part of doing business. 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.

COBIT 5 is based on five key principles for governance and management of enterprise IT detailed below. Together, these principles enable the enterprise to build an effective governance and management framework that optimises information and technology investment and use for the benefit of stakeholders.
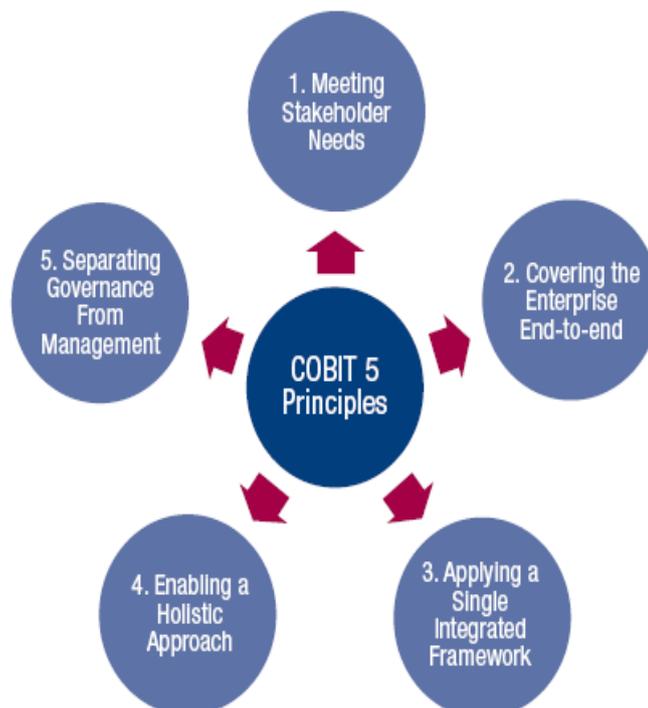
Principle 1: Meeting Stakeholder Needs:

Enterprises exist to create value for their stakeholders by maintaining a balance between the realisation of benefits and the optimisation of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customise COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific processes and practices.

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

COBIT 5 integrates governance of enterprise IT into enterprise governance:

- It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
- It considers all IT-related governance and management enablers to be enterprise 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.

Principle 3: Applying a Single, Integrated Framework:

There are many IT-related standards and best practices, each providing guidance on a subset of IT activities. 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.

Principle 4: Enabling a Holistic Approach:

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. The COBIT 5

framework defines seven categories of enablers namely: Principles, Policies and Frameworks; Processes; Organisational Structures; Culture, Ethics and Behaviour; Information; Services, Infrastructure and Application, People, Skills and Competencies.
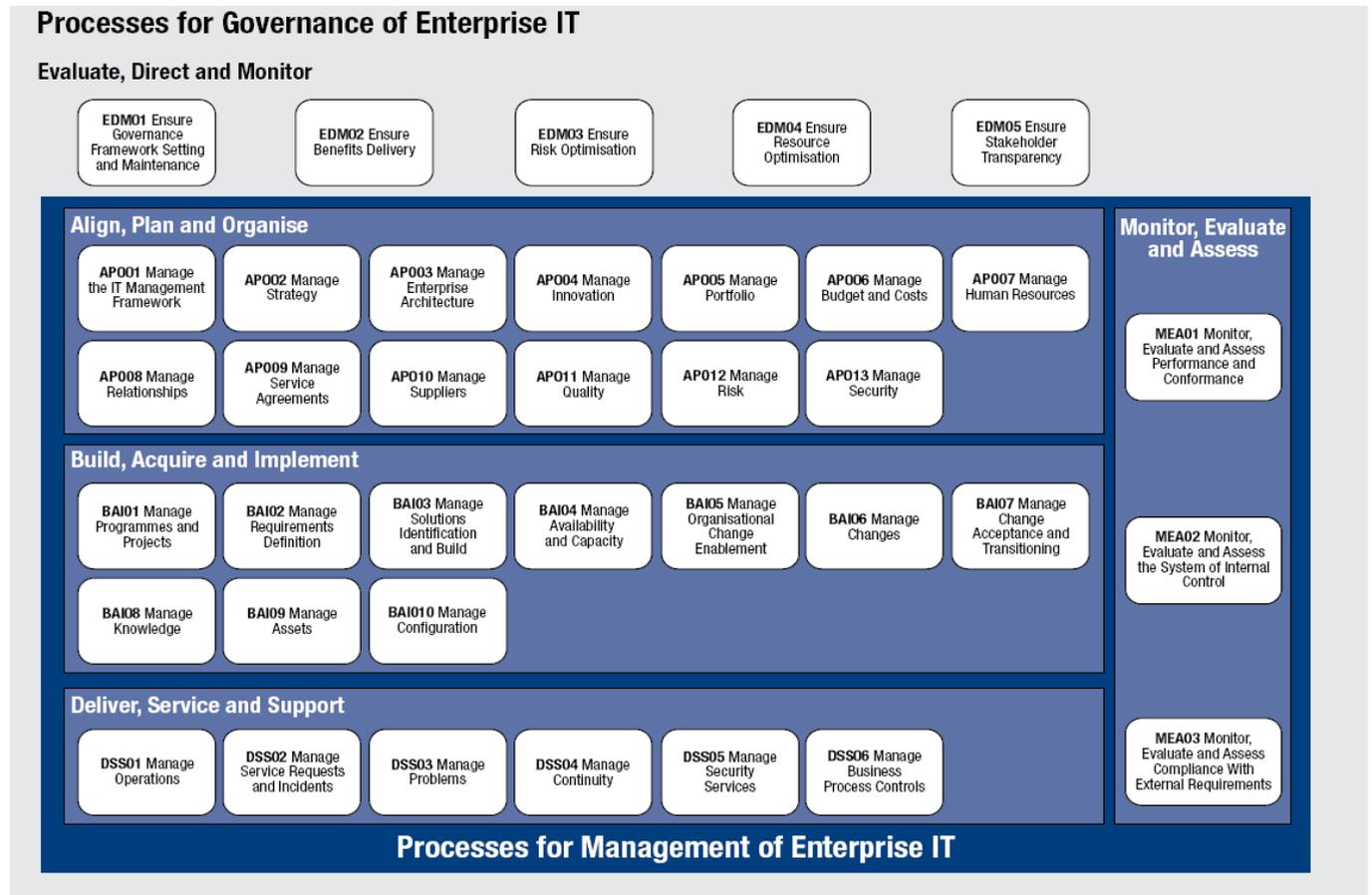
Principle 5: Separating Governance:

From Management—The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organisational structures and serve different purposes. COBIT 5's view on this key distinction between governance and management is:

- 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. In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.

- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

COBIT 5 - Process Reference Model

COBIT 5 includes a process reference model, which defines and describes in detail a number of governance and management processes. It represents all of the processes normally found in an enterprise relating to IT activities, providing common reference model understandable to operational IT and business managers. A process is one of the seven enablers and COBIT is in the process of creating models for the other enablers. In this IT Governance Framework, processes were used as a baseline and the other enablers where taken into account where relevant under the IT related processes identified to be relevant for iLembe to meet its Enterprise goals.

The figure below shows the complete set of 37 governance and management processes within COBIT 5. The details of all processes, according to the process model described previously, are included in a guide entitled COBIT 5: Enabling Processes.

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

| EDM01 Ensure Governance Framework Setting and Maintenance | EDM02 Ensure Benefits Delivery | EDM03 Ensure Risk Optimisation | EDM04 Ensure Resource Optimisation | EDM05 Ensure Stakeholder Transparency |

Align, Plan and Organise

| APO01 Manage the IT Management Framework | APO02 Manage Strategy | APO03 Manage Enterprise Architecture | APO04 Manage Innovation | APO05 Manage Portfolio | APO06 Manage Budget and Costs | APO07 Manage Human Resources |
| APO08 Manage Relationships | APO09 Manage Service Agreements | APO10 Manage Suppliers | APO11 Manage Quality | APO12 Manage Risk | APO13 Manage Security | |

Build, Acquire and Implement

| BAI01 Manage Programmes and Projects | BAI02 Manage Requirements Definition | BAI03 Manage Solutions Identification and Build | BAI04 Manage Availability and Capacity | BAI05 Manage Organisational Change Enablement | BAI06 Manage Changes | BAI07 Manage Change Acceptance and Transitioning |
| BAI08 Manage Knowledge | BAI09 Manage Assets | BAI010 Manage Configuration | | | | |

Deliver, Service and Support

| DSS01 Manage Operations | DSS02 Manage Service Requests and Incidents | DSS03 Manage Problems | DSS04 Manage Continuity | DSS05 Manage Security Services | DSS06 Manage Business Process Controls |

Monitor, Evaluate and Assess

| MEA01 Monitor, Evaluate and Assess Performance and Conformance |
| MEA02 Monitor, Evaluate and Assess the System of Internal Control |
| MEA03 Monitor, Evaluate and Assess Compliance With External Requirements |

Processes for Management of Enterprise IT

6. COBIT Heat map

APPENDIX A - Business Priorities to IT Goals Results - COBIT Heat map link.

uMfolozi IT
Governance Framewc

7. IT Priority Roadmap

APPENDIX B – IT Priority Roadmap.

uMfolozi IT
Governance Framewc

8. Priority 1 Enablers
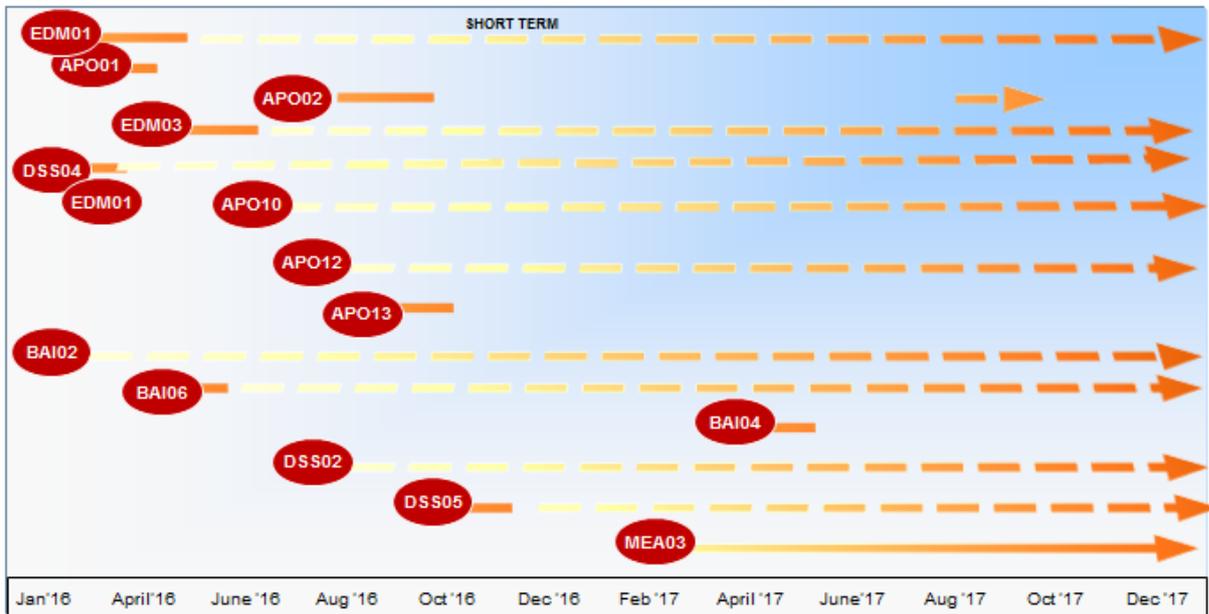
APPENDIX C - Priority 1Enablers for the Organisation.

uMfolozi IT
Governance Framewc

9. Priority Roadmap

IT Governance Framework
Implementation Roadmap – Priority 1 Items (Year 1- 2)

SHORT TERM

EDM01
APO01
APO02
EDM03
DSS04
EDM01
APO10
APO12
APO13
BAI02
BAI06
BAI04
DSS02
DSS05
MEA03

Jan'16   April'16   June'16   Aug'16   Oct'16   Dec'16   Feb'17   April'17   June'17   Aug'17   Oct'17   Dec'17

● Priority 1 Action point

▬ Implementation timeframe   ▬ ▬ ➤ Ongoing Implementation

10. Mapping the IT Governance Framework to KING III

Of particular reference to the development of an IT Governance Framework is Chapter 5 of the King III Code on Corporate Governance which sets forth seven guiding principles for IT Governance. Those recommended practices supporting the principles which are specifically addressed by the contents of the IT Governance Framework are marked with a ✓ . − Denotes elements of the IT Governance Framework that contribute partially to alignment with the King III recommended practices. The respective section of the framework addressing KING III areas is specified under 'Section'.

Principle 1: Board responsibility

Recommended practices	Indicator	Section
The Board should assume the responsibility for the governance of IT and place it on the board agenda.	✓	EDM01
The Board should ensure that an IT charter and policies are established and implemented.	✓	APO01
The Board should ensure promotion of an ethical IT governance culture and awareness and of a common IT language.	−	EDM01.02
The Board should receive independent assurance on the effectiveness of the IT internal controls.		Not being addressed
The Board should receive independent assurance on the effectiveness of the IT internal controls.	−	MEA03.03

Principle 2: Performance and Sustainability

Recommended practices	Indicator	Section
The Board should ensure that the IT strategy is integrated with the company's strategic and business processes.	✓	APO02
The Board should ensure that there is a process in place to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT	−	BAI02

Principle 3: IT Governance Framework

Recommended practices	Indicator	Section
Management should be responsible for the implementation of the structures, processes and mechanisms for the IT Governance Framework.	✓	EDM01
The Board may appoint an IT steering committee or similar function to assist with its governance of IT.	✓	APO01
The CEO should appoint a Chief Information Officer responsible for the management of IT.	✓	APO01
The CIO should be a suitably qualified and experienced person who should have access and interact regularly on strategic IT matters with the board and/or appropriate board committee and executive management.	−	APO01.05

Principle 4: IT Investments

Recommended practices	Indicator	Section
The Board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.	🟡	APO05.03
The Board should ensure that intellectual property contained in information systems are protected		Not applicable
The Board should obtain independent assurance on the IT governance and controls supporting outsourced IT services.	✅	APO10

Note:

It should be noted that some of the KING III IT Governance areas that are not indicated as covered above are already being addressed by the current uMfolozi IT processes

11.   uMfolozi Local Municipality Role Mappings

COBIT and uMfolozi Municipality define different roles within their respective frameworks. For a governance framework, it is essential to have aligned roles in order to create, implement and monitor the Responsibility, Accountability, Consulted and Informed ("RACI") matrix. For the purpose of a complete governance framework, COBIT prescribed roles have been aligned with their overlying uMfolozi IT roles. Thus the role mappings should not be considered equivalent roles, but rather roles whose responsibilities converge. In reality, however, the COBIT roles will be subsets of the uMfolozi roles.

COBIT 5 Roles	uMfolozi IT Roles
Board	**Council**
CEO	**Municipal Manager**
CFO	**CFO**
COO	**Municipal Manager**
Business Executives	**Directors**
Business Process Owners	**Managers**
Strategy Executive Committee	**Executive Committee**
Steering(Programs/Projects) Committee	**IT Steering committee**
Project Management office	**IT Manager**
Value management office	**IT Manager**
Chief Risk Officer	**Risk Management Officer**
Chief Information Security Officer	**IT Manager**
Architecture Board	**IT Steering Committee**
Enterprise Risk Committee	**MANCO Risk Committee**
Head Human Resources	**Human Resources Manager**
Compliance	**Internal Audit**
Audit	**Internal Audit**
Chief Information Officer	**Director Corporate Services**
Head Architect	**IT Manager**
Head Development	**IT Manager**

COBIT 5 Roles	uMfolozi IT Roles
Head IT Operations	**Systems Administrator**
Head IT Administration	**Systems Administrator**
Service Manager	**ICT Security Officer**
Information Security Manager	**ICT Security Officer**
Business Continuity Manager	**Manager: Disaster Management**
Privacy Officer	**ICT Security Officer**