Joe
Morolong
Local
Municipality

IT Governance Framework

RE UNGWELWA ROTLHE

JOE MOROLONG
LOCAL MUNICIPALITY

INDEX

1 Introduction………………………………………………………………………………

2 Contextual background…………………………………………………………

2.1 The CobiT 5 framework (2012) ....

2.2 The ISO 27000 series (2005, 2011)..

2.3 The Risk IT framework (2009) ....

2.4 The King III Report and Code (2009) ....

2.5 Integrated Development Plan ....

2.6 Public sector regulatory environment ....

2.7 The IT regulatory environment ....

2.8 Existing municipal wide governance ....

3 IT governance roles and responsibilities …………………………

.

3.1 IT decision making rights and responsibilities ………………………………………

3.2 IT governance structure………………………………………………………..

3.3 Responsibilities relating to IT Governance…………………………………………..

Introduction

Background

Information Technology (IT) in all its forms have become essential to manage the transactions, information and knowledge necessary to ensure that citizens' demand for service delivery and administrative and operational efficiencies are mat. IT is so pervasive that it is essential for Joe Morolong Local Municipality ("JMLM") to ensure that the function delivers its intended benefits, that risks are managed and that its resources are managed efficiently.

Council and management commitment to IT governance

The Council fully subscribes to the principles of good IT governance as set out in this document (the IT governance framework). The council is accountable for the governance of information technology; however, it has delegated this responsibility to IT Steering Committee and to IT Management.

The essential components of IT governance

It governance is predominantly about making decisions around IT whether it is about strategy, risk, resource management or other issues. This type of decision making is documented in an IT governance framework and made real through IT governance committees (e.g. IT steering committee).

IT governance is also given effect in day to day operations through people, process and technologies (known as IT controls). The design of controls is formalised through IT risk assessments, IT internal control frameworks and IT policies, procedures, standards and plans.

The following table further expands on IT governance components.

IT governance components	Description	Relevant standards
IT governance framework (sometimes referred to as an IT charter)	This provides the foundation, context and structure for IT governance as well as the roles, responsibilities and decision making rights. The municipal goals and the legislative environment have a significant impact on this component.	King lll, CobiT 5, ISO 38500
IT governance committees	Decisions relating to IT are made at various IT governance committee E.g. IT steering committees. This is the most important	

	element of IT governance.	
IT risk assessment	This is where IT risks are identify and quantified, leading to risk management decision	Risk IT,ISO 27005
IT internal control framework	The internal control framework sets how IT risks will be managed through the deployment of IT controls where this makes business sense. SDM will adopt CobiT 5 as its IT internal control framework and this will be evidenced by a capacity maturity assessment on a cyclic basis.	CobiT 5, ISo 27002
IT policies, procedures, standards and plans	The decisions made in the development of the IT internal control framework is expressed as IT policies, procedures standard and plans	CobiT 5, ISO 27002
Information Security Management System	The ISMS is a lifecycle approach to manage security. This is documented as part of the IT policies and procedures.	ISO27001
Day to day operations	This is where people, process and technology come together to make IT governance a reality.	

(2.) Contextual background

The way that IT governance is designed is affected by several factors.

- Several authoritative IT governance frameworks currently exist of which CobiT, King III the ISO 27000 series and Risk IT are dominant within South Africa. These frameworks suggest good practices.
- The municipal strategy and the nature of the organisation will define which areas of IT governance should be implemented first if the municipality is to achieve its goals and stakeholder expectations.
- The regulatory environment will define IT governance elements that must be implemented.
- Municipal wide governance provides the overall framework in which IT governance is to be established. IT governance practices must therefore be aligned to these practices.
- The Auditor General has certain expectations regarding IT controls, which is communicated through audits.

An analysis was conducted of the impact of each of these areas on IT governance focus areas (refer to the sections that follow for supporting detail). This proves the need to progress maturity of IT governance practices through this IT governance framework.

Governance focus area	Industry framework					Regulatory Environment			
	Cobit 5 (SDM)	ISO 27000 series	Risk IT	King 3	IDP	Municipal laws/regulations	IT laws and regulations	Municipal governance	Auditor General
IT governance Committees	x			x	x	x		x	x
IT Risk, Controls and audit	x		x	x	x	x		x	x
IT Strategy				x	x	x			
IT Organisation	x			x					
IT Budget and Investment	x			x	x	x		x	
IT Projects				x					
System Development				x					
IT Suppliers				x			x	x	x
Disaster Recovery	x			x					
Information Security	x	x		x	x	x	x		x
IT Service Delivery	x				x	x			
IT Legal Complience	x			x		x	x		

(2.1) The CobiT 5 framework (2012)

Background

The CobiT (Control Objectives for IT) framework was first developed in the 1990's and it has since positioned itself as the de-facto IT governance framework. It is currently in use by over 140,000 IT governance professionals worldwide. CobiT version 5 has recently superseded CobiT 4.1 and therefore SDM will adopt CobiT 5 as its **IT internal control framework**.

Both CobiT 4.1 and CobiT 5 is based on the assumption that business goals should drive IT governance. CobiT 4.1 had 5 goals (shown in the table hereunder) and CobiT 5 has now consolidated these into 3. However, they are essentially the same between each version of CobiT.

CobiT 5
Bearing on IT governance
IT governance committees
IT risk, controls and audit IT
Strategy
IT organisation
IT budget and investment
IT projects
System development
IT suppliers
Disaster recovery
Information security
IT service delivery
IT legal compliance

Benefits realisation	**Strategic alignment**
Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.	**Focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.**
	Value delivery **Is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on Optimising costs and proving the intrinsic value of IT.**
Risk optimisation **Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to the enterprise value related to the use of IT is identified and managed.**	**Risk management** Requires risk awareness by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the
Resource optimisation Ensure that adequate and sufficient IT-related capabilities (people, process and technology)	**Resource management** Is about the optimal investment in, and the proper management of, critical IT resources:

CobiT 5 IT governance objectives (3)	**CobiT 4.1 IT governance objectives (5)**
Are available to support enterprise objectives at optimal cost.	Applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure. Performance measurement Tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

COBIT 5 provides a framework to assist SDM to achieve these goals through the effective governance and management of enterprise IT. Amongst others, CobiT 5 has an IT process model consisting of 5 domains. The first domain deals with governance and the remaining four domains deals with the management of IT in the typical plan, build, run and monitor lifecycle.

CobiT 5 is aligned with the ISO 38500 IT governance standard, as well as the COSO enterprise risk management framework.

CobiT 5 process model

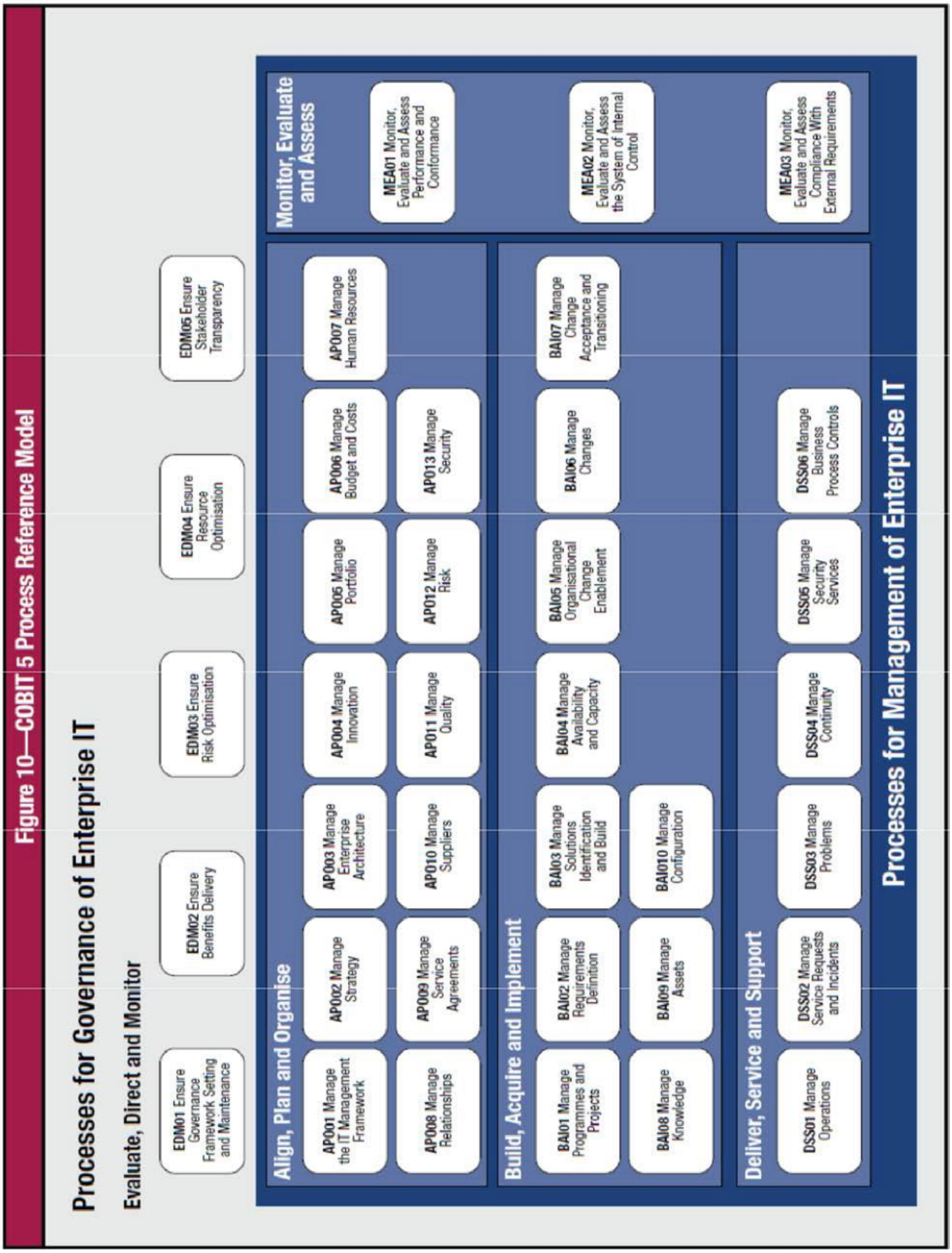


Figure 10—COBIT 5 Process Reference Model

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

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

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

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

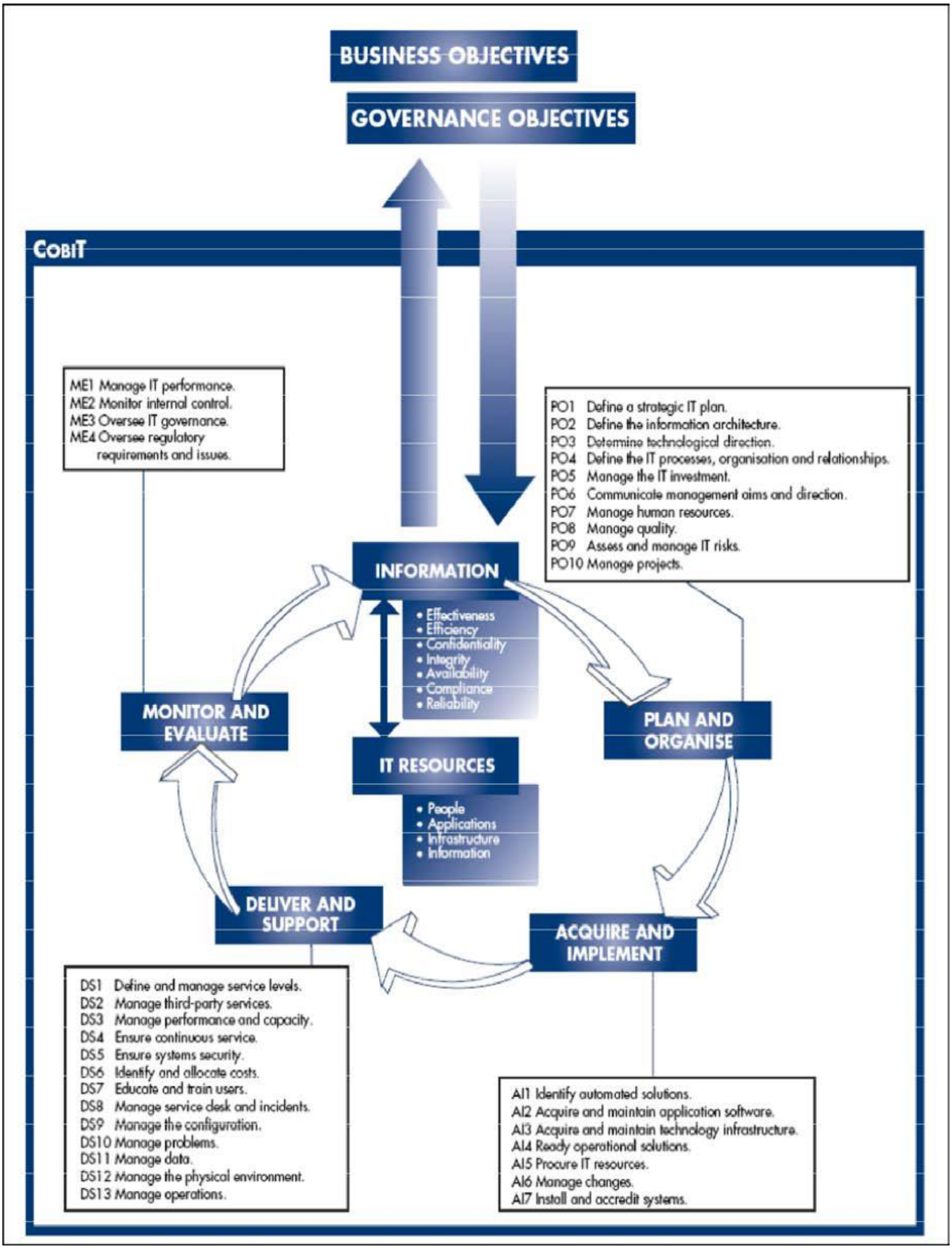
DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

CobiT 4.1 process model



BUSINESS OBJECTIVES
GOVERNANCE OBJECTIVES
COBIT
ME1 Manage IT performance.
ME2 Monitor internal control.
ME3 Oversee IT governance.
ME4 Oversee regulatory requirements and issues.
PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.
INFORMATION
• Effectiveness
• Efficiency
• Confidentiality
• Integrity
• Availability
• Compliance
• Reliability
MONITOR AND EVALUATE
PLAN AND ORGANISE
IT RESOURCES
• People
• Applications
• Infrastructure
• Information
DELIVER AND SUPPORT
ACQUIRE AND IMPLEMENT
DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.
AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Ready operational solutions.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit systems.

CobiT 5 business goals analysis

CobiT 5 allows an organisation to prioritise its CobiT 5 implementation by prioritising a generic set of 17 Business Goals. Each of the 17 Business Goals are mapped to various CobiT 5 processes.
At the point in time of drafting the IT Governance Framework, the following ratings represented the relative importance of each Business Goal with 10 being the most important and 1 being the least important to SDM.

Balanced Scorecard domain	**Business Goal**	**Score** 1 to 10
FINANCIAL	1. STAKEHOLDER VALUE OF BUSINESS INVESTMENTS	**6**
	2. PORTFOLIO OF COMPETITIVE PRODUCTS AND SERVICE	1
	3. MANAGED BUSINESS RISKS (SAFEGUARDING OF ASSETS)	9
	4. COMPLIENCE WITH EXTERNAL LAWS AND REGULATIONS	10
	5. FINANCIAL TRANSPARENCY	9
	6. CUSTOMER ORIENTED SERVICE CULTURE	8
	7. BUSINESS SERVICE CONTINUITY AND AVAILABILITY	7
CUSTOMER	8. AGILE RESPONSE TO A CHANGING BUSINESS ENVIRONMENT	2
	9. ONFORMATION BASED STRATEGIC DECISION MAKING	8
	10. OPTIMISATION OF SERVICE DELIVERY COSTS	8
	11. OPTIMISATION OF BUSINESS PROCESS FUNCTIONALITY	7
	12. OPTIMISATION OF BUSINESS PROCESS COSTS	8
INTERNAL	13. MANAGED BUSINESS CHANGE PROGRAMMES	8
	14. OPERATIONAL AND STAFF PRODUCTIVITY	10
	15. COMPLIANCE WITH INTERNAL POLICIES	10
LEARNING AND GROWTH	16. SKILLED AND MOTIVATED PEOPLE	10
	17. PRODUCT AND BUSINESS INNOVATION CULTURE	5

Although it is not a precise science, the table on the previous page roughly results in the following prioritisation of IT processes.

		CobiT 5 process	SCORE 1 - 10
Monitor, Direct and Evaluate	EDMO1	Ensure Governance framework setting and maintenance	8
	EDMO2	Ensure Benefits Delivery Ensure	
	EDMO3	Risk Optimisation Ensure Resource	6
	EDMO4	Optimisation	10
	EDMO5	Ensure Stake Holder Transparency Management	8
	AP001	Manage the IT Management Framework	8
Align, Plan and Organise	AP002	Manage Strategy	10
	AP003	Manage Enterprise Architecture	6
	AP004	Manage Innovation	5
	AP005	Manage Portfolio	3
	AP006	Manage Budget and Cost	6
	AP007	Manage Human Resource	9
	AP008	Manage Service Agreements	10
	AP009	Manage Suppliers	6
	AP0010	Manage Quality	6
	AP0011	Manage Risk	6
	AP0012	Manage Security	6
	BAI01	Manage Programmes and Projects	10
Build, Acquire and Operate	BAI02	Manage Requirements Definitions	10
	BAI03	Manage Solutions and Identifications and Build	8
	BAI04	Manage Availability Capacity	7
	BAI05	Manage Organisational Change Enablement	6
	BAI06	Manage Changes	7
	BAI07	Manage Change Acceptance and Transitioning	8
	BAI08	Manage Knowledge	7
	BAI09	Manage Assets	8
	BAI010	Manage Configuration	2
	DSS01	Manage Operation	9
Deliver Service and Support	DSS02	Manage Service Request and Incidents	8
	DSS03	Manage Problems	6
	DSS04	Manage Continuity	6
	DSS05	Manage Security Service	8
	DSS06	Manage Business Process Control	7
	MEA01	Monitor, Evaluate and Assess Performance and	6
Monitoring, Evaluate and Assessments		Conformance	6
	MEA01	Monitor, Evaluate and Assess the System of Internal	10
		Control	10
	MEA03	Monitor, Evaluate and Assess Compliance with External	
		Requirements	10

The above table demonstrates that the most important IT controls for the municipality relates to IT risk management, IT skills development, information security, and IT legal Compliance and IT cost control.

(2.2) The ISO 27000 series (2005, 2011)

After CobiT 5, the ISO 27000 series is currently the most recognised Information Security standard in the world. The most prominent standards in the series are:

- ISO 27001:2005 - A specification for an Information Security Management System (ISMS).
- ISO 27002:2005 - A set of Information Security controls, which is useful to develop Information Security policies.
- ISO 27005:2011 - A standard on how to approach an Information Security risk assessment

ISO 27000 series **Bearing on IT governance**
IT governance committees
IT risk, Controls and audit IT strategy
IT organisation
IT budget and investment
IT projects
System development
IT suppliers
Disaster recovery
Information Security
IT service delivery
IT Legal Compliance

King III and CobiT 5 promote the implementation of an **Information Security Management System** and therefore ISO 27001 is relevant to SDM. An Information Security Management System is simply put a lifecycle process (plan-do-check-act) to manage Information Security. To give effect to the ISO 27000 series, the controls included in ISO 27001 and ISO 27002 will be embedded into the Information Security policies where this makes business sense. ISO 27005 will be used to shape Information Security risk assessments when this is conducted.
ISO 27001 and ISO 27002 are widely used in South Africa and in some large government organisations. Although very few organisations formally certify against the standard, they do familiarise themselves with its content and implement where it makes sense.

ISO 27002:2005 chapters
Risk assessment and treatment
Organisation of information security
Assessment management
Human resource security
Physical and environmental security
Communication operation management
Access control
Information system acquisition, development and maintenance
Information security incident management
Business continuity management
compliance

(2.3) The RiskIT framework (2009)

RiskIT is a well-known framework that is published by the same authors as CobiT 5. RiskIT contains an approach to conduct an IT risk assessment, which includes a ready-made inventory of 36 generic IT risk scenarios that covers the known IT risk universe. RiskIT will be useful as a reference point when conducting an IT risk assessment.

RiskIT Bearing on IT governance
IT governance committees
IT risk, Controls and audit IT strategy
IT organisation
IT budget and investment
IT projects
System development
IT suppliers
Disaster recovery
Information Security
IT service delivery
IT Legal Compliance

The universe of IT risks according to RiskIT		
1. IT programme selection 2. New technologies 3. Technology Selection 4. IT investment decision making 5. Accounting over IT 6. Integration of IT within business process 7. State of infrastructure technology 8. Ageing of application software 9. Architectural agility and flexibility 10. Regulatory Compliance	11. Software implementation 12. IT project Termination 13. IT projects economics 14. Project delivery 15. Project quality 16. Selection/performance of third party suppliers 17. Infrastructure theft 18. Destruction of infrastructure 19 IT staff 20. IT expertise and skills 21. Software integrity 22. Infrastructure (hardware) 23. Software performance	24. System Capacity 25. Ageing of infrastructural software 26. Malware 27. Logical attacks 28. Information media 29. Utilities performance 30. Industrial action 31. Database integrity 32. Logical trespassing 33. Operational IT errors 34. Contractual compliance 35. Environmental 36. Acts of nature

(2.4) The King III Report and Code (2009)

Background

The King Committee on Governance issued the King Report on Governance for South Africa – 2009 (the "Report") and the King Code of Governance Principles – 2009 (the "Code") together referred to as "King III" on 1 September 2009. King III was issued in response to changes to corporate legislation and in international governance trends that have emerged since the release of the second King Report on Corporate Governance for South Africa (King II) in 2002.

The National Treasury Risk Management Framework encourages Municipalities to adhere to the principles espoused in King II, given its promotion of an advanced level of institutional conduct. This suggests an endorsement of its Successor, King III. Notwithstanding, King III itself now asserts that it is explicitly applicable to all types of entities, including Municipalities.

King III (2009)
IT governance committees
IT risk, Controls and audit IT strategy
IT organisation
IT budget and investment
IT projects
System development
IT suppliers
Disaster recovery
Information Security
IT service delivery
IT Legal Compliance

The use of instructive language in King III is important in reading and understanding the Report and the Code. The word 'must' indicates a legal requirement. In aspects where it is believed the application of the Code will result in good governance, the word 'should' is used. The word 'may' indicates areas where certain practices are proposed for consideration. For this reason, the terms 'Company', 'Board' and 'Directors' in King III refer to the functional responsibility of those charged with IT Governance in any entity and is likely read as 'Municipality', 'Council' and 'Councillors' respectively. However, SDM has taken a view that much of the responsibilities of the "Board" and "Directors" will likely be assumed by the Management Committee.

IT governance and King III

King III recognises the critical role that IT has come to play in all organisations, including Municipalities where IT is a key success factor to meet citizens' demand for service delivery, and administrative and operational efficiencies. For this reason, Chapter 5 now deals with IT specifically.

Chapter 5 deals with many issues around IT governance. These include:

- The need for an IT governance framework, IT Charter, IT Steering Committee, IT internal control framework, IT policies, a sufficiently skilled IT function and an IT governance culture.
- The importance of exploiting opportunities to improve the performance and sustainability of the Municipality through the use of IT.
- IT controls such as disaster recovery, Information Security, IT legal compliance, IT outsourcing and project management.
- Audit and Risk committees' responsibility for IT risks, controls and audit.

King III does not address the application of its principles and therefore the Municipality will have to consider the approach that best suits its size and complexity.

The section that follows contains the more precise wording related to King III Chapter 5.

King III extract: 5. the governance of information technology

Principle 5.1: The board should be responsible for information technology (IT) governance.

- The board should assume the responsibility for the governance of IT and place it on the board agenda.
- The board should ensure that an IT charter and policies are established and implemented.
- The board should ensure promotion of an ethical IT governance culture and awareness and of a common IT language.
- The board should ensure that an IT internal control framework is adopted and implemented.
- The board should receive independent assurance on the effectiveness of the IT internal controls.

Principle 5.2: IT should be aligned with the performance and sustainability objectives of the company.

- The board should ensure that the IT strategy is integrated with the company's strategic and business processes.
- The board should ensure that there is a process in place to identity and exploit opportunities to improve the performance and sustainability of the company through the use of IT.

Principle 5.3: The board should delegate to management the responsibility for the Implementation of an IT governance framework.

- Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework.
- The board may appoint an IT Steering Committee of similar function to assist with its governance of IT.

Principle 5.4: The board should monitor and evaluate significant IT investments and expenditure.

- The board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.
- The board should ensure that intellectual property contained in information systems is protected.
- The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services.

Principle 5.4: The board should monitor and evaluate significant IT investments and expenditure.

- The board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.
- The board should ensure that intellectual property contained in information systems is protected.
- The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services.

Principle 5.6: The board should ensure that information assets are managed effectively.

- The board should ensure that there are systems in place for the management of information which should include information security, information management and information privacy.
- The board should ensure that all personal information is treated by the company as an important business asset and is identified.
- The board should ensure that an Information Security Management System is developed and implemented.
- The board should approve the information security strategy and delegate and empower management to implement the strategy.

Principle 5.7: A risk committee and audit committee should assist the board in carrying out its IT responsibilities.

- The Risk Committee should ensure that IT risks are adequately addressed.
- The Risk Committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks.
- The Audit Committee should consider IT as it relates to financial reporting and the going concern of the company.
- The Audit Committee should consider the use of technology to improve audit coverage and efficiency.

(2.5) Integrated Development Plan

The strategic direction of the municipality has a direct bearing on the IT governance framework as priorities are set and IT governance deliverables are defined. The Integrated Development Plan ("IDP") is the key strategic document in SDM which sets a platform for communities, stakeholders, private sectors and non-governmental organisations to meaningfully engage with DM.

The IDP states in its Vision that municipality realises that its core responsibility and mandate is to be developmentally orientated, namely to inspire, encourage and ensure a safe, healthy, educational, economically viable and friendly environment that will enhance and harness a culture of self-reliance amongst the citizens of the Region

IDP **Bearing on IT governance**
IT governance committees
IT risk, Controls and audit IT strategy
IT organisation
IT budget and investment
IT projects
System development
IT suppliers
Disaster recovery
Information Security
IT service delivery
IT Legal Compliance

The SDM strategic objectives are:

- Economic Development
- Infrastructure Development
- Social and Community Development
- Financial Management
- Human Resources Development

The strategic goals, identified in addition to the IDP goals, are the following:

- Integration of planning, systems and processes in order to optimize service delivery
- Shared services and the sharing of expertise by sustained support to local municipalities.
- Effective communication in order to share information internally and externally and to improve morale.
- Identifying and implementing alternative funding resources.
- Improved co-operation between municipalities and other governmental facets.
- Initiating an accountable administration and a repeated unqualified audit opinion.
- Creating an integrated economy-friendly environment, especially for investors and local emerging business communities.
- Promotion of tourism to the Siyanda region by marketing and empowering of local communities.
- Effective infrastructure maintenance and development.
- Managing and protecting assets.
- Motivated and empowered personnel corpse by:

  - ✓ Personnel development (communicating skills to create development opportunities and fill critical positions).
  - ✓ Performance management.
  - ✓ Career planning.

Having analysed the above, there is a substantial requirement placed on the Municipality to align the IT strategy with the IDP, to exploit IT to its fullest and to protect IT assets. There is also emphasis on matters such as IT cost management, service delivery and IT audit.

(2.6) Public sector regulatory environment

There are more than 130 laws and regulations applicable in a direct or indirect way to municipalities or other state organs. The principles of IT governance have not been well established and DM needs to make certain assumptions relating to the public sector regulatory environment on the municipality's IT governance framework.

In summary, the most prominent legislative requirements have the following bearing in IT governance:

- IT resources must be used effectively, efficiently and economically.
- IT assets must be protected.
- IT controls must be audited, using a risk-based approach.
- An IDP must be developed, which should deal with IT strategic matters.
- Personal information must be protected.
- IT governance must be established, using King III and CobiT.
- IT use must improve service delivery to the public.
- IT must be used to make the organisation more productive and cost effective.
- Information security controls must be implemented.

Municipality Laws/Regulations bearings on IT Governance
IT governance committees
IT risk, Controls and audit IT strategy
IT organisation
IT budget and investment
IT projects and Suppliers
System development
Disaster recovery
Information Security
IT service delivery
IT Legal Compliance

Set out below is an extract or brief summary from the relevant acts or regulations:

Acts	**Relevant sections**
Municipal Finance Management Act (MFMA)	62. General financial management functions. – (1) The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure – (a) that the resources of the municipality are used effectively, efficiently and economically; (c) (ii) of internal audit operating in accordance with any prescribed norms and standards; 63. Asset and liability management. – (1) The accounting officer of a municipality is responsible for the management of (a) the assets of the municipality, including the safeguarding and the maintenance of those assets: 165 internal audit unit (2) The internal unit of municipality or municipality entity must – (a) Prepare a risk based audit plan and internal program fr each financial year (b) Advise accounting officer and report to the audit committee the implementation of the internal audit plan and matters relating to- (i) internal audit, controls (ii) accounting procedures and practices; (iii) risk and risk management; (iv) performance management; (v) loss control; and (vi) compliance with this Act, the annual Division of Revenue Act and any other applicable legislation; and 166 Audit committees (2) An audit committee is an independent advisory body which must- advise the municipal council, the political office-bearers, the accounting officer and the management staff of the municipality or board of directors entity on matters relating to- (i) Risk management (ii) The adequacy, reliability and accuracy of financial reporting and information

Municipal Structure Act	26. Core components of integrated developments plans – An integrated developments plans must reflect – (1) the councils operation strategies:
Constitution	The right to privacy is enshrined in the Constitution and gives effect to this right by way of mandatory procedures and mechanisms for the handling and processing of personal information, in line with current international trends and laws in privacy
Public service regulations	Chapter 5 (1) (B) places the obligations on the head of the institution to ensure that acquisition, management and use of information technology by the institution improves. (a) Direct or indirect service delivery to the public including but not limited to, equal aces by the public to services delivered by the institution (b) The productivity of the institution and cost efficiency of the institution
Minimum information security standards (written by the National Intelligence Agency and published by DPSA)	The head of every institution bears overall the responsibility for the provision and maintenance of security of his her institution. This is however have to be delegated to the head of the security components within the organisation
IT PLANNING **Guidelines provide & adopted by the government information and technology officers committee in 2002**	Provides guidance to the public sector organisation on how to align IT Objectives to the overall organizational strategy. Refers to the CobiT as a Framework
National Treasury Risk Management Framework	The framework promotes King ii as an advanced level of institution conduct. It can reasonably assumed that King lll will be endorsed I the same way in the future revisions of the framework. King lll deals with the council responsibility for IT governance within its charter 5

(2.7) The IT regulatory environment

The IT regulatory environment places certain requirements on the way that SDM governs its IT function. A snapshot of relevant legislation is set out below:

- Copyright Act 98 of 1978
- Electronic Communications and Transactions Act 25 of 2002
- Electronic Communications Security (Proprietary) Limited Act 68 of 2002
- National Archives and Record Service of South Africa Act 43 of 1996
- Promotion of Access to Information Act 2 of 2000
- Protection of Information Act 84 of 1982
- Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
- Trade Marks Act 194 of 1993
- The Merchandise Marks Act 17 of 1941
- Protection of Personal Information Bill

IT laws and regulations Bearing on IT governance
IT governance committees
IT risk, Controls and audit IT strategy
IT organisation
IT budget and investment
IT projects and Suppliers
System development
Disaster recovery
Information Security
IT service delivery
IT Legal Compliance

This legislation predominantly affects Information Security controls within SDM. The legislation also affects the way SDM deals with its suppliers and the general public.

(2.8) *Existing Municipal wide governance*

The existing enterprise wide municipal governance is developed to comply with the relevant legislation. This will have bearing on several areas such as:

- Council
- Administration
- External stakeholders, including wards and other spheres of government
- Enterprise wide risk management
- By-laws and policies

Municipal governance Bearing on IT governance
IT governance committees
IT risk, Controls and audit
IT strategy
IT organisation
IT budget and investment
IT projects and Suppliers
System development
Disaster recovery
Information Security
IT service delivery
IT Legal Compliance

(3) *IT governance roles and responsibilities*

(3.1) IT decision making rights and responsibilities

This section defines the core decision making rights, roles and responsibilities for IT governance within Municipality. As stated earlier, IT governance is predominantly about making decisions around IT. In order to formalise IT decision making, the decision making domains have to be identified and then mapped to the decision making bodies. The following areas were therefore identified that have bearing on the use of IT within the municipality.

Decision Making Domain		Guidance	IT Governance Objectives		
1	IT Governance	• IT governance framework (IT decision-making • structures, principles, processes and practices) • IT internal control framework • IT policies, procedures, standards and plans • Compliance with IT-related laws and regulations • Adoption of industry IT standards, rules, codes, • frameworks and good practices • Exceptions against IT governance • Performance of the IT function	Benefits Realisation	Risk Optimisation	Resource Optimisation
2	IT Strategy and Sourcing	• Longer-term positioning of IT services to support the • IDP • Introduction of new technologies and approaches	x	x	x
3	IT Applications and Infrastructure	• Application acquisition, maintenance, replacement • and consolidation • Architecture standards and	x	x	x

		principles, as well as • compliance thereof • Infrastructure acquisition, maintenance and retirement • Outsourcing of IT services			
4	Information	• Information lifecycle management • Data ownership and classification			x
5	IT Budget	• Prioritisation of IT expenditure and projects • IT budgets and financial controls	x		X
6	Bids	• Specification and evaluation criteria, as well as awarding of bids	x		X
7	IT Risk	• IT risk practices, treatment strategies and / or risk acceptance without treatment • IT risk appetite thresholds		x	
8	Security	• Security strategies, practices and technologies • Security awareness culture		x	

The following decision making structures would be responsible for each kind of decision.

Decision making domain	EMC	ITSC	ITM	HoDs	SCM	AC	RMC
1 IT Governance	A	R	R,C			C,I	
2 IT Strategy and Sourcing		R	R,C				
3 IT Applications and Infrastructure		R	R,C				
4 Information		R	R,C	A,R			
5 IT Budget		R	R,C				
6 Bids		C			A,R		
7 IT Risk		R	R,C	A		I	C,I
8 Security		A,R		A,R			

Legend		

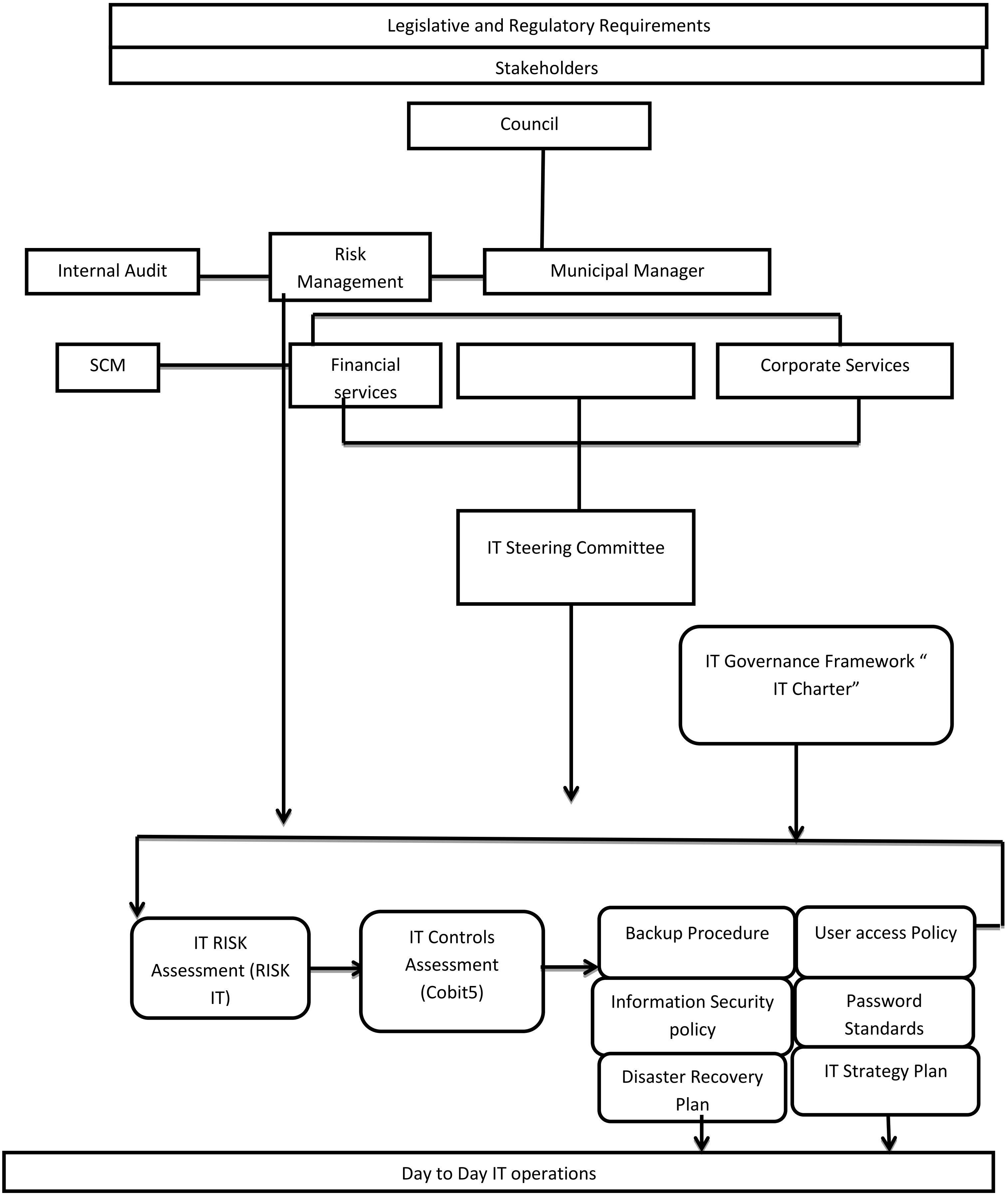
EMC = Executive Mayoral Committee	HoDs = Heads of Departments
	SCM = Supply Chain Management
		A=Accountable
		R=Responsible

ITSC = IT Steering Committee	AC = Audit Committee	C=Consulted

ITM = IT Manager	RMC = Risk Management Committee	I=Informed

(3.2) **IT governance structure**

The following illustration represents the IT governance structure for the district municipality:



(3.3) Responsibilities relating to IT Governance

The Committees will have the following responsibilities for IT Governance:

IT governance structure	Decision making domain	Responsibilities
Executive Mayoral Committee	IT Governance	✓ Has overall accountability for IT governance and exceptions to IT governance ✓ Approve the IT Governance Framework ("IT Charter"). ✓ Approve the IT internal control framework and other industry, standards, rules, codes, frameworks and good practice. ✓ Approved IT policies.
Municipal Manager	IT Governance	✓ Approve the IT governance framework, IT internal control framework and any industry standards, rules and codes of good IT practice that have been adopted. ✓ Promote an awareness of the benefits of IT governance within the municipality. ✓ Approve IT policies, procedures, standards and plans. ✓ Satisfy itself that the IT function complies with IT related laws. ✓ Approve exceptions against established IT governance. ✓ Set performance targets for the IT function and establish a monitoring approach. ✓ Review the performance of the IT function.
	IT strategy and sourcing	✓ Promote awareness among Directors / functions of IT products and services, and the importance of exploiting IT to meet municipal objectives ✓ Understand stakeholder requirements for the IT function. ✓ Develop an IT strategy (technological direction and tactical plans) that aligns with the municipal IDP SDBIP. ✓ Continuously evaluate the IT function (skills – sets, investments, assets and service) to determine the likelihood of it supporting the municipal objectives at reasonable cost. Support changes in direction when deemed necessary. ✓ Oversee that IT strategy and its

IT Steering Committee	IT Applications and Infrastructure	implementation. ✓ Ensure that Directorates / functions understand the importance of having common IT software and hardware standards ✓ Approve IT standards, technology innovations or other changes to enterprise application. Ensure that the municipality has an effective disaster recovery plan. Ensure that a change control process is established for application and infrastructure changes.
	IT Budget	✓ Approve the IT budget. ✓ Monitor how well IT spend and IT investment are aligned to the municipal IDP and SDBIP ✓ Ensure that IT spend present an acceptable balance of sustaining and renewing the Municipality's IT function.
	IT Governance	✓ Ensure that an IT governance framework ("IT Charter") is developed and implemented. ✓ Assess the effectiveness of the IT governance framework design on a periodic basis. ✓ Promote an awareness of the benefits of IT governance within the municipality. ✓ Ensure that an IT internal control framework is adopted and implemented. ✓ Ensure that industry IT standards, rules, codes, frameworks and good practice are identified and considered on a continuous basis and that IT policies are reviewed and adjusted accordingly. ✓ Ensure that IT policies, procedures, standards and plans are ✓ Defined, maintained and implemented.
	Applications and Infrastructure	✓ Ensure that IT-related laws and regulations are identified on a ✓ Continuous basis and that IT policies are reviewed and adjusted accordingly. ✓ Ensure that the organisation honours its IT contracts. ✓ Review the performance of the IT function. ✓ Ensure that IT standards are established and promote the ✓ implementation of technology innovations and changes to enterprise applications ✓ Ensure that Directorates / functions understand the importance of having common IT hardware and software

		standards. ✓ Ensure that the municipality has an effective disaster recovery plan. ✓ Ensure that a change control process is established for application and infrastructure changes.
	Information	✓ Ensure that HODs and IT Management develop and implement Information Management practices.
	IT Budget	✓ Assist with the development of the IT budget. ✓ Monitor how well IT spend and IT investment are aligned to the municipal IDP and SDBIP. ✓ Ensure that IT spend present an acceptable balance of sustaining and renewing the Municipality's IT function.
	Bids	✓ Ensure that cost-efficient IT solutions and services are delivered by the IT function. ✓ May be consulted by Supply Chain Management on IT related procurement.
	IT Risk	✓ Ensure that practices are established that will ensure that risks affecting municipal objectives - related to its use of IT - are identified and managed within the municipal risk appetite thresholds. ✓ Ensure that decisions relating to the treatment or acceptance of risk are proposed. ✓ Ensure that IT and municipal-wide risk management practices are aligned. ✓ Ensure that an IT control framework to mitigate IT risks is adopted. ✓ Monitor the extent to which the IT risk profile is managed within the municipal risk appetite thresholds. ✓ Ensure that IT policies are adjusted in accordance with risk treatment or acceptance decisions.
	Security	✓ Ensure that Information Security policies, procedures, standards and plans are developed, maintained and implemented. ✓ Ensure that the Municipality stays abreast of Information Security trends and industry good practice (such as the information security management system good

IT Governance	IT Governance IT Strategy and Sourcing IT Strategy and Sourcing	practice), and IT policies (in particular the information security policy) are reviewed and adjusted accordingly. ✓ Ratify HODs' decisions relating to Security. ✓ Promote a culture of security awareness within the municipality to ensure that everyone is aware of their responsibility relating to Information Security. ✓ Develop, maintain and implement an IT Governance Framework ("IT Charter") ✓ Adopt an IT internal control framework and ensure its implementation. ✓ Define, maintain and implement IT policies, procedures, standards and plans. ✓ Identify and consider IT standards, rules, codes, frameworks and good practices are identified and considered on a continuous basis and that IT policies are reviewed and adjusted accordingly. ✓ Ensure that IT-related laws and regulations are identified on a ✓ Continuous basis and that IT policies are reviewed and adjusted accordingly ✓ Honour commitments within IT contracts. ✓ Enable review of the status and initiatives around IT governance within Municipality by the Management Committee and the IT Steering Committee. ✓ Enable a review of the performance of the IT function by the ✓ Management Committee and the IT Steering Committee. ✓ Understand stakeholder requirements for the IT function. ✓ Promote awareness among Directorates / functions of IT products and services, and the importance of exploiting IT to meet municipal objectives. ✓ Assist with the development of an IT strategy (technological direction and tactical plans) that aligns with the municipal IDP SDBIP. ✓ Enable review of the IT strategy implementation by the IT Steering Committee. ✓ Understand stakeholder requirements for

			the IT function. ✓ Promote awareness among Directorates / functions of IT products and service, and the importance of exploiting IT to meet municipal objectives ✓ Assist with the development of an IT strategy (technological direction and tactical plans) that aligns with the municipal IDP SDBIP. ✓ Enable review of the IT strategy implementation by the IT Steering Committee.
	IT Application and Infrastructure		✓ Establish and maintain IT standards as well as promote the ✓ Implementation of technology innovations and changes to enterprise applications. ✓ Promote awareness with Directorates / functions of the importance of having common IT hardware and software standards. ✓ Develop and test a disaster recovery plan for the municipality. ✓ Establish a change control process for application and infrastructure changes
	Information		✓ Assist HODs with the development and implementation of Information Management practices.
	IT Budget		✓ Assist with the development of the IT budget. ✓ Ensure that IT spend present an acceptable balance of sustaining and renewing the Municipality's IT function. ✓ Enable a reliable and accurate view of IT costs and IT projects by the IT Steering Committee and Management Committee. ✓ Deliver cost-efficient IT solutions and services.
	IT Budget		✓ Establish practices that will ensure that risks affecting municipal objectives - related to its use of IT - are identified and managed within the municipal risk appetite thresholds. ✓ Propose decisions relating to the treatment or acceptance of risk. ✓ Align the IT and municipal-wide risk

		management practices. ✓ Adopt an IT control framework to mitigate IT risks. ✓ Enable review of the IT risk profile and major IT risks by stakeholders and committees with accountability or responsibility for IT risks. ✓ Monitor the extent to which the IT risk profile is managed within the municipal risk appetite thresholds. ✓ Review IT policies and adjust in accordance with risk treatment or acceptance decisions.
Heads of Department	Information Management	✓ Develop and implement Information Management practices.
	IT Risk	✓ Ensure that practices are established to manage IT risk within the municipal risk appetite thresholds. ✓ Monitor the extent to which the IT risk profile is managed within the municipal risk appetite thresholds. ✓ Promote a culture, and educate municipal management, to ensure IT-risk aware municipal-wide decision making.
	Security	✓ Establish practices to protect municipal information and IT assets from security threats. ✓ Develop, maintain and implement Information Security policies, procedures, standards and plans. ✓ Stay abreast of Information Security trends and industry good practice and those IT policies are reviewed and adjusted accordingly. ✓ Promote a culture of security awareness within the municipality to ensure that everyone is aware of their responsibility relating to Information security. ✓ Enable review of security vulnerabilities, incidents and the current status of Information Security controls, by the IT Steering Committee.
Supply Chain Management	Bids	✓ Ensure that IT procurement follows Supply Chain Management governance. ✓ Awarding of bids.
Audit Committee	IT Risks	✓ Informed of the IT risk profile and

Risk Management Committee	IT Risk	whether it is within the municipal risk - appetite thresholds ✓ Review independent assurance that IT controls are in place and sufficient to address IT risks. ✓ Ratify decisions relating to the treatment or acceptance of risk. ✓ Informed of the IT risk profile and whether it is within the municipal risk appetite thresholds. ✓ Review independent assurance that IT controls are in place and sufficient to address IT risks.