Municipal Corporate Governance of ICT Policy

Date Approved	Version	Resolution Number
30 June 2016	1	10.3.2
28 July 2017	2	019/OCM/17

The Information Technology Manager

Senqu Local Municipality

19 Murray Street

Lady Grey

Telephone (051) 603 1300

Facsimile (051) 603 0445

Website: www.senqu.gov.za

Resolution 019/OCM/17 Approved 28 July 2017

Municipal Corporate Governance of ICT Policy

Information and Communications Technology (ICT) Governance has been described as the effective and efficient management of ICT resources to facilitate the achievement of organisational goals and objectives. ICT does not exist for its own sake within an organisation; ICT is there to make sure that organisations achieve sustainable success through the use of their ICT. ICT is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's ICT (the infrastructure as well as the capabilities and organisation that is established to support ICT) sustains and extends the organisation's strategies and objectives.

Full Title	**Senqu Municipality's IT Security Control Policy**
Short Title	IT Security Control Policy
Author(s)	Mr R Johl

Resolution:019/OCM/17 Approved 28 July 2017

Table of Contents

1. Version Control

Full Title	**Senqu Municipality Municipal Corporate Governance**
Short Title	MCGICT Policy
Author(s)	Mr N Suleman
Version	0.1

Authors	Mr N Suleman (PWC) & Ms. Magdalena Oertel (Senqu)
Version	01
Authorised By	Council
Authorisation Date	30 June 2016
Effective Date	1 July 2016

Revised	Ms. Magdalena Oertel (Senqu Municipality)
Version	02
Authorised By	Council
Authorisation Date	28 July 2017
Effective Date	1 July 2017

2. Definitions

Term	Meaning
CFO	Chief Financial Officer
COBIT	Control Objectives for Information Technology
Municipality, the	Senqu Municipality
EXCO	Executive Committee
GICTF	Governance of Information and Communication Technology Framework
GITO	Government Information Technology Officer
MM	Municipal Manager
ICT	Information Communication and Technology
IM	Information Management
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	The Information Technology Infrastructure Library
PRINCE2	PRojects IN Controlled Environments (Project Management Frameworks)
RFI	Request for Information
RFP	Request for Proposal
SALGA	South African Local Government Association
SLA	Service Level Agreement

3. Introduction

IT Governance is defined as a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management.

IT Governance can be further defined as the process by which IT decisions are made and incorporate how decisions are made, who makes decisions, who is held accountable and how the results of the decisions are measured and monitored.

IT Governance is the responsibility of Senior Management and consists of the leadership, Municipal structures and processes that ensure that the Municipality's IT business unit sustains and extends the Municipality's strategies and objectives.

3.1 Corporate Governance in Municipalities:

Corporate governance is a vehicle through which value is created within a municipal context. Value creation means realising benefits while optimising resources and risks. This value creation takes place within a governance system that is established by the municipal policy. A governance system refers to all the means and mechanisms that enable the Municipality's Council and Management team to have a structured and organised process.

3.2 Corporate Governance of IT in Municipalities:

The Corporate Governance of IT is an integral part of the corporate governance system in municipalities. The Corporate Governance of IT involves evaluating, directing and monitoring the alignment of the IT strategy with the Municipality's IDP and related strategies. The Corporate Governance of IT also involves the monitoring of IT service delivery to ensure a culture of continuous IT service improvement exists at the Municipality. The Corporate Governance of IT includes determining IT strategic goals and plans for IT service delivery as determined by the Service Delivery and Budget Implementation Plan (SDBIP) objectives of the Municipality.

4. Purpose

The purpose of this policy is to institutionalise the Corporate Governance of IT as an integral part of corporate governance within the Municipality in a uniform and coordinated manner. This policy provides a set of principles and practices which will assist to institutionalise the Corporate Governance of IT.

5. Scope/Audience

This Policy has been developed to guide and assist the Municipality to be aligned with the Corporate Governance of ICT best practice frameworks. This Policy therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective Corporate Governance of ICT.

6. Role of the IT business unit

The Municipal Manager will appoint a suitably qualified and experienced IT Manager. The IT Manager has the responsibility to manage the IT business unit which will serve Senqu Municipality.

The objectives of the IT business unit are as follows:

6.1 To ensure that the IT Strategy is aligned to the Municipality's strategy. Opportunities to improve the use of IT within Senqu Municipality are identified and exploited. That optimal investment is made in IT, costs are managed and the return on investment is measured.
6.2 Synergies between IT initiatives are enabled and IT choices are in the best interest of the Municipality as a whole and not only those of individual business units.
6.3 IT services are sourced optimally and legitimately.
6.4 IT risks are identified and adequately addressed. Assurance is obtained to ensure that an IT control framework is in place to address IT risks.
6.5 Information, IT assets and intellectual property contained in IT systems are protected and effectively managed and used.
6.6 IT has adequate business resilience arrangements in place for disaster recovery.
6.7 Information management is a joint IT and business responsibility.
6.8 IT use conforms to IT related laws and related rules, codes and standards.
6.9 IT use is sustainable with respect to the environment.

7. Municipal Corporate Governance of IT Policy Objectives

The objective of this Corporate Governance of IT Policy for the Municipality seeks to achieve the following:

7.1 Institutionalising a Corporate Governance of IT Policy that is consistent with the Corporate Governance Framework of the Municipality.
7.2 Aligning the IT strategic goals and objectives with the Municipality's strategic goals and objectives.
7.3 Ensuring that optimum Municipal value is realised from IT-related investment, services and assets.
7.4 Ensuring that Municipal IT-related risks do not exceed the Municipality's risk appetite and risk tolerance.
7.5 Ensuring that IT-related resource needs are met in an optimal manner by providing the organisational structure, capacity and capability.
7.6 Ensuring that communication with stakeholders is transparent, relevant and timely.
7.7 Ensuring transparency of performance and conformance and driving the achievement of strategic goals through monitoring and evaluation.

8. Benefits of Good Governance of IT

When Corporate Governance of IT is effectively implemented and maintained, the following benefits will be realised:

8.1 Establishment of IT as a strategic enabler in the Municipality.
8.2 Improved achievement of municipal integrated development plans.
8.3 Improved effective service delivery through IT-enabled access to municipal information and services.
8.4 Improved IT enablement of the Municipality.
8.5 Improved delivery of IT service quality.
8.6 Improved stakeholder communication.
8.7 Improved trust between the municipality and the community through the use of IT.
8.8 Lower costs for IT functions and IT dependent functions.
8.9 Increased alignment of IT investment towards municipal integrated development plans.
8.10 Improved return on IT investments.
8.11 IT risks managed in line with the IT priorities and risk appetite of the Municipality.
8.12 Appropriate security measures to protect both the Municipality and its employee's information.
8.13 Improved management of municipal-related IT projects.

8.14 Improved management of information as IT is prioritised on the same level as other resources in the Municipality.

8.15 IT pro-actively recognises potential efficiencies and guides the Municipality in timeous adoption of appropriate technology.

8.16 Improved IT ability and agility to adapt to changing circumstances.

8.17 IT executed in line with legislative and regulatory requirements.

9. Legislative Framework

The Municipality must be aware of and comply with the legislative landscape applicable to its environment. This includes the following:

- Local Government Municipal Systems Act, Act 32, of 2000, Local Government: Municipal Structures Act, Act 117 of 1998.
- Public Administration Management Act, Act 11 of 2014.
- Local Government: Municipal Finance Management Act, Act 56 of 2003.

This policy has been developed with the following sections of legislation in mind:

9.1 In terms of the **Municipal Systems Act, Act 32, of 2000, Section 55(1)**:

"The Municipal Manager of a Municipality is, subject to the policy directions of the municipal council, responsible and accountable for:

(a) The formation and development of an economical effective, efficient and accountable administration:

(i) Equipped to carry out the task of implementing the municipality's integrated development plan in accordance with Chapter 5:
(ii) Operating in accordance with the municipality's performance management system in accordance with Chapter 6;"

9.2 In terms of the **Municipal Finance Management Act, Act 56 of 2003, Section 62**:

"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.
(b) That full and proper records of the financial affairs of the municipality are kept in accordance with any prescribed norms and standards;"

9.3 In terms of the **Municipal Finance Management Act, Act 56 of 2003, Section 78**, the Act stipulates that:

"Each Senior Manager of a Municipality and each official of a Municipality exercising financial management responsibilities must take all reasonable steps within their respective areas of responsibility to ensure:

(a) That the system of financial management and internal control established for the Municipality is carried out diligently;
(b) That the financial and other resources of the Municipality are utilised effectively, efficiently, economically and transparently;

(c) That any unauthorised, irregular or fruitless and wasteful expenditure and any other losses are prevented;"

10. Corporate Governance of IT Good Practices and Standards

In recognition of the importance of IT Governance, a number of internationally recognised frameworks and standards will be adopted to provide context for the institutionalisation of the governance of IT.

10.1 The **King III Code:** The most commonly accepted Corporate Governance Framework in South Africa is also valid for municipalities. It was used to inform the Governance of IT principles and practices and to establish the relationship between Corporate Governance of and Governance of IT.

10.2 **ISO/IEC 38500:** Internationally accepted as the standard for Corporate Governance of IT; IT provides governance principles and a model for the effective, efficient, and acceptable use of IT within the Municipality.

10.3 **Municipal Corporate Governance of Information and Communication Technology Policy:** The purpose of the Municipal Corporate Governance ICT Policy is to institutionalise the Corporate Governance of ICT as an integral part of corporate governance within municipalities. This Municipal Corporate Governance ICT Policy provides the Municipal Council and Management within a municipality with a set of principles and practices that must be complied with, together with an implementation approach to be utilised for implementation of ICT Governance within Municipalities.

10.4 **Other** internationally accepted process frameworks for implementing Governance of IT.

11. Layered Approach to Corporate Governance of IT in Municipalities

11.1 Corporate Governance of IT encompasses two levels of decision-making, authority and accountability to satisfy the expectations of all stakeholders. These levels are:

11.1.1 Facilitating the achievement of the Municipality's strategic goals (Corporate Governance of IT).
11.1.2 The efficient and effective management of IT service delivery (Operational Governance of IT).

11.2 The implementation of Corporate Governance of IT in the Municipality thus consists of the following layered approach:

11.2.1 This Municipal Corporate Governance of IT Policy, which addresses the Corporate Governance of ICT layer at a strategic level.
11.2.2 Other best practice frameworks which will be adapted to give effect to the governance of the IT operational environment within the Municipality.

12. IT Governance Framework Components

The figure below illustrates the IT Governance Framework that has been adopted by Senqu Municipality. Each of the components of the IT Governance Framework is discussed in detail in the following sections.

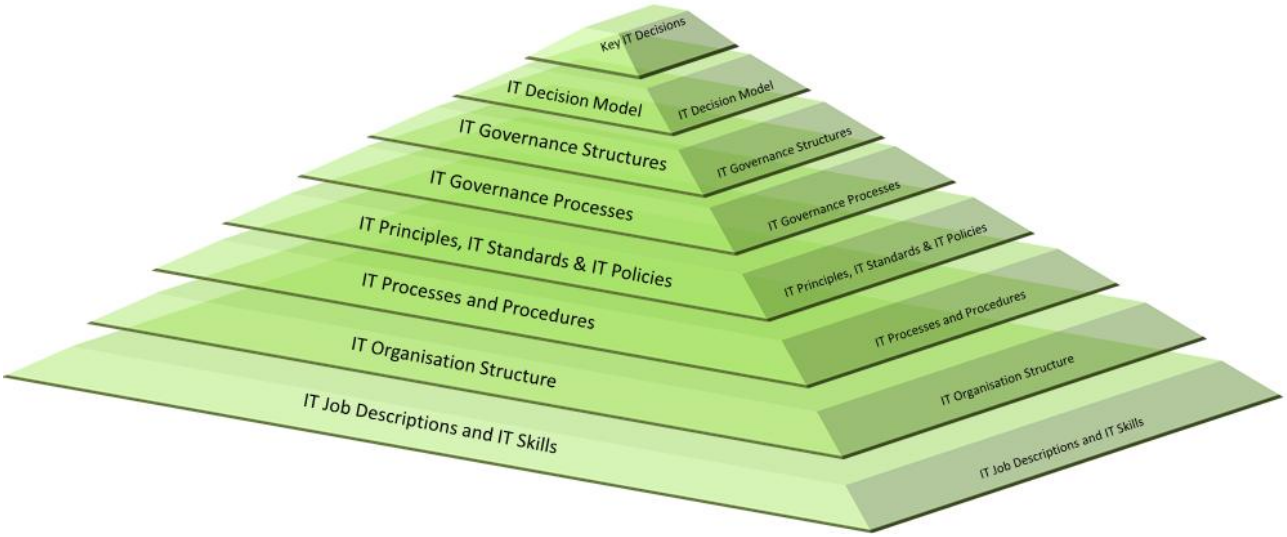

Figure 1: IT Governance Framework

12.1 Key IT Decisions

12.1.1 Introduction and Objective

The objective of this section is to identify and define the key IT decisions that typically need to be made within Senqu Municipality.

12.1.2 Implementation Guidance and Minimum Requirements

The following IT decision categories are adopted by Senqu Municipality:

12.1.2.1 IT Governance, Risk and Compliance.
12.1.2.2 IT Strategy.
12.1.2.3 Application Management.
12.1.2.4 Information.
12.1.2.5 Business and IT Architecture.
12.1.2.6 IT Investments and Projects.
12.1.2.7 IT Sourcing.
12.1.2.8 IT Security.
12.1.2.9 IT Operations.
12.1.2.10 General IT Management and Administration.
12.1.2.11 IT Change Management.

For each specific decision, the Municipality must consider the following:

- The frequency of the decision (ad-hoc, annually).
- The information required to make the decision.
- Prerequisites for the decision to be made.
- Impacts on other decision domains.
- Specific limitations on the scope of decisions.

12.1.2.1 IT Governance, Risk and Compliance

IT governance structures, processes, principles, procedures and standards must ensure adequate risk management, compliance with legal requirements and ensuring the optimal use of information and IT in support of the Municipality's strategy.

Decisions in this domain include:

12.1.2.1.1 IT governance structures (committees).
12.1.2.1.2 Roles and responsibilities.
12.1.2.1.3 IT principles, procedures and standards.
12.1.2.1.4 IT governance processes (e.g. managing exceptions).
12.1.2.1.5 IT risk management framework that documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks.
12.1.2.1.6 Translating IT governance arrangements into operational IT structures and processes across all domains.
12.1.2.1.7 Change management with respect to IT governance arrangements.
12.1.2.1.8 IT financial governance (e.g. sign-off levels, budget principles such as depreciation rules).

12.1.2.2 IT Strategy

Identification and positioning of strategic IT initiatives and services which will best contribute to the achievement of the Municipality's strategic objectives and are agile and adaptive enough to support changes in the Municipality's strategy.

Decisions in this domain include:

12.1.2.2.1 Business relationship management.
12.1.2.2.2 The approval of the IT strategy.
12.1.2.2.3 Ensuring that there is sufficient alignment with the Municipality strategy and that it sets the right direction for IT within the Municipality.
12.1.2.2.4 Implementation of the IT strategy and monitoring of the outcomes and conflicting priorities.

12.1.2.3 Application Management

The management of the development, configuration, implementation, hosting, support and maintenance of applications.

Decisions in this domain include:

12.1.2.3.1 The acquisition, development, and implementation of applications, (e.g. the system development lifecycle to be utilised, development languages and procedures, license management).
12.1.2.3.2 The hosting, support and maintenance of applications.

12.1.2.4 Information

Ensuring Municipal and IT alignment with respect to the structuring, acquisition, control, protection, delivery and value enhancement of data and information assets to the Municipality.

Decisions in this domain include:

12.1.2.4.1 Information lifecycle policies and procedures, from creation to destruction, of both electronic and hard-copy documents.
12.1.2.4.2 Custodianship of data and information.
12.1.2.4.3 Access to information (including information security levels).
12.1.2.4.4 Information classification.

12.1.2.5 Business and IT Architecture

Enterprise architecture across all domains (business, information, data, application and technology) and technology platforms to support the agility and change imposed by the Municipality when required.

Decisions in this domain include:

12.1.2.5.1 Architecture migration planning and change management.
12.1.2.5.2 Standards for all domains and asset classes.
12.1.2.5.3 Monitoring of compliance to standards and principles.
12.1.2.5.4 Exceptions to defined architecture standards and principles.
12.1.2.5.5 Approving solution architectures per project initiatives, vendor assessments, service level agreements and RFI/RFP documentation from an architecture point-of-view.
12.1.2.5.6 Research and innovation in terms of IT trends and emerging technologies.

12.1.2.6 IT Investments and Projects

Prioritise, approve, co-ordinate, control and monitor the operational and capital IT budget and the associated implementation and delivery of projects.

Decisions in this domain include:

12.1.2.6.1 The size of and process for determining the overall IT budget.
12.1.2.6.2 The prioritisation and approval of IT investment requests ensuring the right balance between initiatives that run the current business, grow the existing business, and have the potential to transform the business.
12.1.2.6.3 The definition of investment thresholds by the various decision making bodies.
12.1.2.6.4 The allocation of resources to approved initiatives.
12.1.2.6.5 Project management principles and frameworks.
12.1.2.6.6 Monitoring IT investment outcomes and realisation of benefits.

12.1.2.7 IT Sourcing

Optimal sourcing processes and strategies for IT commodities and IT services and the approval of significant procurement from suppliers.

Decisions in this domain include:

12.1.2.7.1 Review and approval of IT sourcing strategies within specific IT services or IT commodity categories.
12.1.2.7.2 Approval of the procurement process and the approach to manage supplier delivery.
12.1.2.7.3 Approval and oversight of significant contracts relating to the procurement from suppliers.

12.1.2.8 IT Security

Protection of the integrity and availability of information, data and assets. Authorisation for authorised users, personnel and systems to access information in a secure and protected manner.

Decisions in this domain include:

12.1.2.8.1 Information Security Management System design and implementation.
12.1.2.8.2 Security risk appetite.
12.1.2.8.3 Security policies, principles and standards.
12.1.2.8.4 Security operations across all asset classes and domains.
12.1.2.8.5 Allocation of security resources to supplement asset classes and domains.

12.1.2.9 IT Operations

Delivery of required services, which includes service delivery, management of security and continuity, service support for users and management of data and operational facilities.

Decisions in this domain include:

12.1.2.9.1 Operational level agreements with other business units.
12.1.2.9.2 The acquisition and implementation of infrastructure.
12.1.2.9.3 The management and support of this infrastructure.
12.1.2.9.4 Disaster recovery in terms of IT business continuity execution.

12.1.2.10 General IT Management and Administration

IT management practices such as human resources, finance and marketing.

Decisions in this domain include:

12.1.2.10.1 The IT organisation structure as well as roles and responsibilities.
12.1.2.10.2 The financial management of IT.
12.1.2.10.3 The marketing of IT.
12.1.2.10.4 Human resource development and management.

12.1.2.11 IT Change Management

IT Change Management is the practice of ensuring the delivery of IT and municipal services is not impacted by infrastructure or software changes and that all changes are recorded and carried out in a planned and authorised manner.

Decisions in this domain include:

12.1.2.11.1 Reviewing the reason/justification for the change.
12.1.2.11.2 Approval of changes to infrastructure or software changes.
12.1.2.11.3 Risks of implementing or not implementing the change.
12.1.2.11.4 Identifying the IT services and systems affected by the change.
12.1.2.11.5 Identifying the staff/third party/supplier involvement in the implementation of the change.
12.1.2.11.6 Communication mechanism to be used among stakeholders.
12.1.2.11.7 The impact on non-IT infrastructures within the Municipality.
12.1.2.11.8 Technical capability and technical approval.
12.1.2.11.9 Review/assessment of the change priority.

12.2 IT Decision Model

12.2.1 Introduction and Objective

The objective of this section is to determine which stakeholders need to be involved in each of the decision domains as well as to determine the role each stakeholder will play when a decision is to be made based on the types of key IT decisions defined in section 12.1.

12.2.2 Implementation Guidance and Minimum Requirements

When developing the decision model for each decision category, the type of involvement that is required from each stakeholder must be documented. The various roles that a stakeholder could have when participating in decision making are as follows:

12.2.2.1 **Responsible** for a decision: The stakeholder making the decision to achieve the deliverable.

12.2.2.2 **Accountable** for a decision: The stakeholder ultimately answerable for the decision that has been made and the one who delegates the work to those responsible.

12.2.2.3 **Consulted** during a decision: Stakeholders whose opinions are sought when making a decision. These are typically subject matter experts and with whom there is two-way communication.

12.2.2.4 **Informed** about a decision: Stakeholders who are kept up-to-date on progress, often only on completion of the project or deliverable and with whom there is just one-way communication.

Senqu Municipality stakeholders involved in the IT decision model are as follows:

- Municipal Manager
- IT Manager
- CFO
- Top Management Committee
- EXCO
- Audit and Performance Committee

The decision model adopted by Senqu Municipality is depicted in Table 1 overleaf.

Table 1: IT Decision Model

IT Decision Category	Formal Decision Making Body	Municipal Manager	IT Manager	CFO	Top Management Committee	EXCO	Audit and Performance Committee
IT Governance, Risk and Compliance	IT Steering Committee	A	R	I	I	I	C
IT Strategy	IT Steering Committee	A	R	I/C	C	C	I
Application Management	IT Steering Committee	A	R	C	C	I	I
Information	IT Steering Committee	A	R	I	C	I	I
Business and IT Architecture	IT Steering Committee	A	R	I	C	C	I
IT Investments and Projects	IT Steering Committee	A	R	C	C	I	I
IT Sourcing	IT Steering Committee	A	R	C	I	I	I
IT Security	IT Steering Committee	A	R	I	I	I	C
IT Operations	IT Steering Committee	A	R	I	I	I	I
General IT Management and Administration	IT Steering Committee	C	A/R	I	I	I	I
IT Change Management	IT Steering Committee	A	R	I	I	I	I

Key:

R = Responsible
A = Accountable
C = Consulted
I = Informed

12.3 IT Governance Structures

12.3.1 Introduction and Objective

IT governance structures establishes the strategic, operational, and technical decision-making process required to ensure IT enables Senqu Municipality to excel in its mission. The objective is to establish decision making bodies or committees, membership of these committees, the responsibilities they will assume and how these bodies interact with each other.

12.3.1.1 Implementation Guidance and Minimum Requirements

For each governance structure, it must be clearly documented what responsibilities the structure has, the composition of the structure as well as the relationship and interaction between other governance structures, frequency of meetings, communication lines and quorums to be able to make decisions.

12.3.1.2 IT Steering Committee

An IT Steering Committee must be established by Senqu Municipality and must take oversight responsibility for making decisions with regard to the following IT decision categories:

12.3.1.2.1 IT Governance, Risk and Compliance.
12.3.1.2.2 IT Strategy.
12.3.1.2.3 Application Management.
12.3.1.2.4 Information.
12.3.1.2.5 Business and IT Architecture.
12.3.1.2.6 IT Investments and Projects.
12.3.1.2.7 IT Sourcing.
12.3.1.2.8 IT Security.
12.3.1.2.9 IT Operations.
12.3.1.2.10 General IT Management and Administration.
12.3.1.2.11 IT Change Management.

The IT Steering Committee will have a direct communication line to Top Management Committee and an indirect communication line to the Audit and Performance Committee.

The relationship between the Municipality's' governance structures for reporting are illustrated in the figure below.

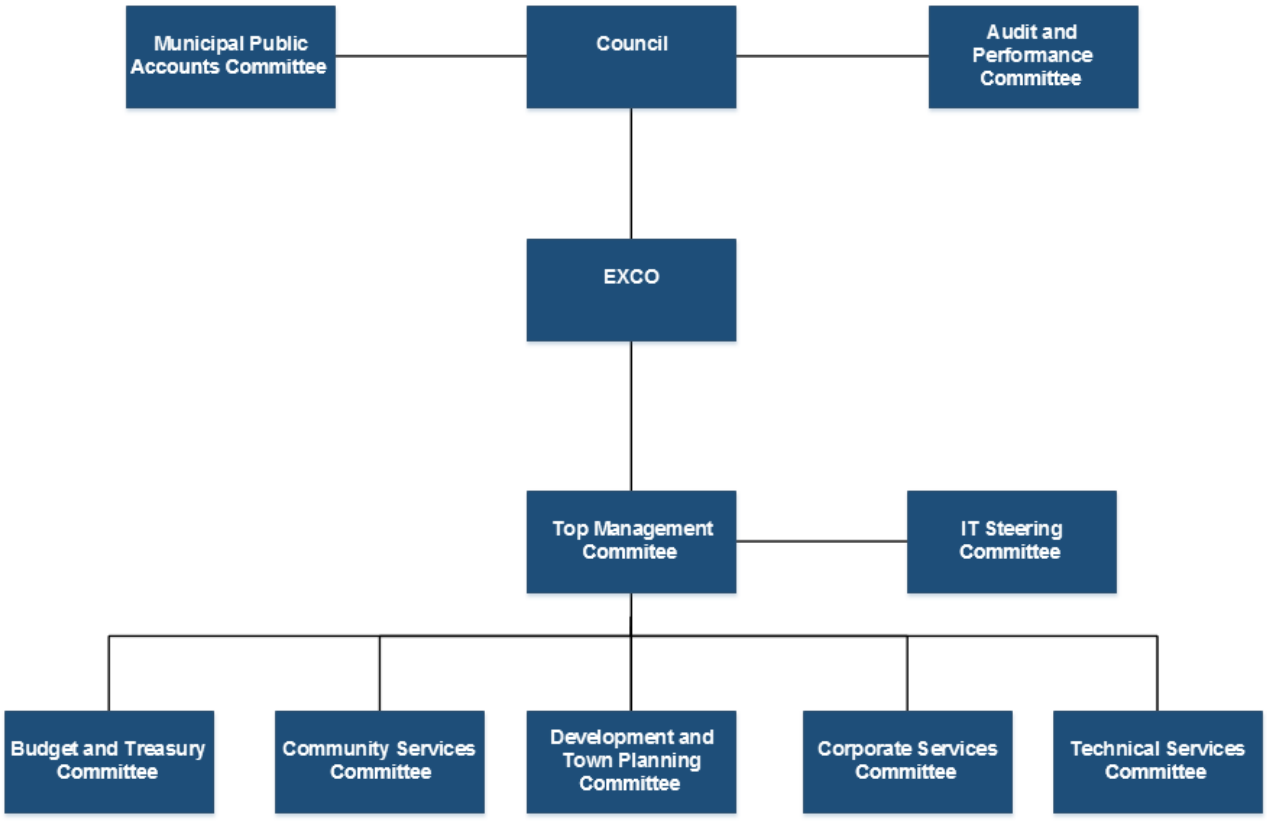

Figure 2: Governance Structure Relationships

12.4 IT Governance Processes

12.4.1 Introduction and Objective

IT Governance processes are required to be implemented to facilitate and enable the IT Governance Framework on a day-to-day basis. The processes below will form part of the framework.

12.4.2 Implementation Guidance and Minimum Requirements

12.4.2.1 Management of Exceptions

This is a documented and structured mechanism for stakeholders to state their case and request exceptions to defined policies, standards and principles. It also includes the activities that are followed to escalate requests that are deemed to be required but have been rejected.

Refer to Appendix A1 for details on the process flow.

12.4.2.2 Management of Risk

IT risk management is the process of identifying IT risks, assessing these risks and taking steps to reduce risk to an acceptable level. Risk management is an essential function of the Municipality, and therefore IT risk management must integrate with the Municipality's overall risk management process.

The objective of the risk management process is to allow IT management to balance the benefits and costs of protective measures and to support the strategic objectives by adequately protecting all IT assets that support the Municipality's strategic objectives.

Refer to Appendix A2 for details on the process flow.

12.4.2.3 Agreement and Management of Service Levels

The main objective of the service level and agreement process is to enable the delivery of reliable, responsive, effective and efficient IT services, that meets the Municipality's requirements as precisely as possible.

Service level agreements represent the internal contract between the IT business unit and other business units. SLA's often result in improved behavior from business units – by exposing the IT impact of their business requirements and requests for services, the business units have an improved understanding of the IT environment, its resources and constraints. The SLA is usually based on a Service Catalogue (SC) which lists available IT services, alternative quality levels and related costs. The negotiation of the

SLA is an important governance process since it leads to increased business/IT alignment through greater clarity on Municipal requirements. It also leads to improved sourcing decisions. Once requirements are explicitly stated in a detailed form, comparison can be made between internal service provisioning and outsourced options.

Refer to Appendix A3 for details on the process flow.

12.5 IT Principles, IT Practices, IT Standards and IT Policies

12.5.1 IT Principles

12.5.1.1 Introduction and Objective

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which the Municipality sets about fulfilling its mission.

12.5.1.2 Implementation Guidance and Minimum Requirements

Below are the guiding Corporate Governance of IT Principles that have been adopted by Senqu Municipality. These principles are based on the principles described in the Municipal Corporate Governance of ICT Policy.

Table 2: Municipal Corporate Governance of IT Principles

No.	Principle	Description
1	**Political Mandate** The Governance of IT must enable the municipality's political mandate.	The Municipal Council must ensure that Corporate Governance of IT achieves the service delivery mandate of the municipality.
2	**Strategic Mandate -** The Governance of IT must enable the municipality's strategic mandate.	The Municipal Manager must ensure that Corporate Governance of IT serves as an enabler to the municipality's strategic plans.
3	**Corporate Governance of IT** The Municipal Manager is responsible for the Corporate Governance of IT.	The Municipal Manager must create an enabling environment in respect of the Corporate Governance of IT within the applicable legislative and regulatory landscape and information security context.
4	**IT Strategic Alignment** IT service delivery must be aligned with the strategic goals of the municipality.	Management must ensure that IT service delivery is aligned with the municipal strategic goals and that the administration accounts for current and future capabilities of IT. IT must ensure that IT is fit for purpose at the correct service levels and quality for both current and future Municipal needs are met.
5	**Significant IT Expenditure** Management must monitor and evaluate significant IT expenditure.	Management must monitor and evaluate major IT expenditure, ensure that IT expenditure is made for valid Municipal enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed.
6	**Risk Management and Assurance** Management must ensure that IT risks are managed and that the IT function is audited.	Management must ensure that IT risks are managed within the municipal risk management practice. IT must also ensure that the IT function is audited as part of the municipal audit plan.

7	**Organisational Behaviour** Management must ensure that IT service delivery is sensitive to organisational behaviour/culture.	Management must ensure that the use of IT demonstrates the understanding of and respect for organisational behaviour/culture.

12.5.2 IT Practices

12.5.2.1 Introduction and Objective

The following practices, outlined in Table 3 below, have been assigned to specific designated municipal structures and officials in order to achieve the objectives and principles contained in this Municipal Corporate Governance of ICT Policy:

Table 3: Municipal Corporate Governance of IT Policy Practices

No.	Practice Description
1.	**The Municipal Council must:** Provide political leadership and strategic direction through: a. Determining policy and providing oversight. b. 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 municipality to leverage ICT as an enabler of the municipal IDP. c. Assist the Municipal Manager to deal with intergovernmental, political and other ICT-related Municipal issues beyond their direct control and influence. d. Ensure that the municipality's organisational structure makes provision for the Corporate Governance of ICT.
2.	**The Municipal Manager must:** a. Provide strategic leadership and management of ICT. b. Ensure alignment of the ICT strategic plan with the municipal IDP. c. Ensure that the Corporate Governance of ICT is placed on the municipality's strategic agenda. d. Ensure that the Corporate Governance of ICT Policy, charter and related policies for the institutionalisation of the Corporate Governance of ICT are developed and implemented by management. e. Determine the delegation of authority, personal responsibilities and accountability to Management with regards to the Corporate Governance of ICT. f. Ensure the realisation of municipality-wide value through ICT service delivery and management of Municipal and ICT-related risks. g. Ensure that appropriate ICT capability and capacity are provided and a suitably

No.	Practice Description
	qualified and experienced Governance Champion is designated. h. Ensure that appropriate ICT capacity and capability are provided and that a designated official at a Management level takes accountability for the Management of ICT in the municipality. i. Ensure the monitoring and evaluation of the effectiveness of the Corporate Governance of ICT system through the IT steering committee.
3.	**The Municipal IT Steering Committee and the Audit and Performance Committee must:** a. Assist the Municipal Manager in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.
4.	**Management must ensure:** a. ICT strategic goals are aligned with the Municipality's strategic goals and support the municipal processes. b. Municipal-related ICT strategic goals are cascaded throughout the municipality for implementation and are reported on.

12.5.3 IT Standards

12.5.3.1 Introduction and Objective

A standard is defined as a document established by consensus and approved by a recognised body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

The figure overleaf depicts the different layers of governance and the interrelationship between the different Frameworks and Standards adopted by the Municipality. All of the frameworks reflected in the figure below are generally accepted frameworks. King III is the corporate governance standard adopted by most entities in South Africa and the other standards like ISO, ITIL, PRINCE2 and COBIT are internationally recognised frameworks and standards operating at different levels within the IT Governance Framework.

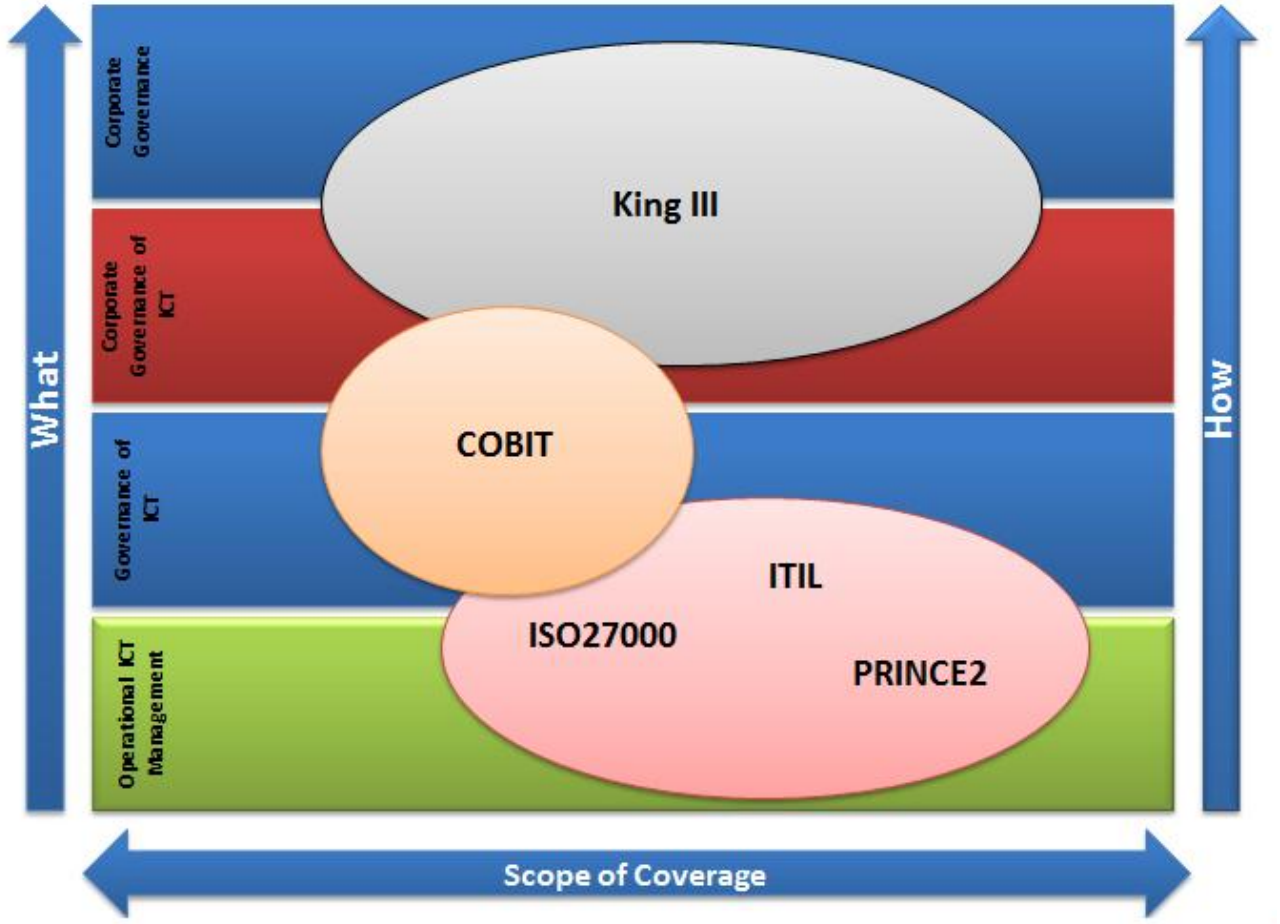

Figure 3: Interrelation between adopted Codes, Frameworks and Standards

12.5.3.2 Implementation Guidance and Minimum Requirements

Figure 3 above reflects the frameworks, standards and codes that have been used to develop the IT Governance Framework. The standards, frameworks and codes reflected in Figure 3 are internationally recognised or generally accepted standards. Table 4 overleaf provides a general description of each standard or framework which has been adopted by Senqu Municipality.

Table 4: IT Frameworks and Standards

Framework/ Standard	Description
King III	King III Code is a Code of Good Governance emphasising corporate leadership, business sustainability and corporate citizenship. The King III Code is the most commonly accepted corporate governance framework in South Africa and is also valid for the public sector.
COBIT	COBIT is an internationally accepted process framework for the implementation of the governance of IT. COBIT fully supports the principles of the King III Code and the ISO 38500 standard on the corporate governance of ICT. Principle 5.1.3 of the King III Report on Governance recommends that an IT internal control framework be adopted and implemented.
ISO/IEC 27002	ISO/IEC 27002 is a code of practice for information security management. It can be used by any organisation that needs to establish a comprehensive information security management program or improve its current information security practices. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).
ITIL	The Information Technology Infrastructure Library (ITIL) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. It provides a practical framework for identifying, planning, delivering and supporting IT services to the business. It will provide guidance to the Municipality on how to use IT as a tool to facilitate business change, transformation and growth.
PRINCE2	PRINCE2 (an acronym for PRojects IN Controlled Environments) is a de facto process-based method for effective project management. Used extensively by the UK Government, PRINCE2 is also widely recognised and used in the private sector, both in the UK and internationally. The PRINCE2 method is in the public domain and offers non-proprietorial best practice guidance on project management. PRINCE2 will be adopted and used for managing projects within the Municipality.

12.5.4 IT Policies

12.5.4.1 Introduction and Objective

Policies are approved at the highest level of the Municipality and are designed to remain in effect regardless of changes in people, technology or the mission of the Municipality. The need for policies is driven by the Municipality's objectives, resource requirements, organisational risks, rules and legislation and the maturity level of the Municipality. It also provides guidance for standards, processes and procedures, controls and structures.

12.5.4.2 Implementation Guidance and Minimum Requirements

The following IT policies will be adopted by the Municipality:

12.5.4.2.1 Municipal Corporate Governance of ICT Policy
12.5.4.2.2 IT Governance Charter
12.5.4.2.3 IT Risk Management Policy
12.5.4.2.4 IT Internal Audit Plan
12.5.4.2.5 IT Management Policy
12.5.4.2.6 IT Project and Portfolio Management Policy
12.5.4.2.7 IT Disaster Recovery Plan
12.5.4.2.8 Data Backup and Recovery Policy
12.5.4.2.9 IT Service Level Agreement Management Policy
12.5.4.2.10 IT User Access Management Policy
12.5.4.2.11 IT Security Controls Policy
12.5.4.2.12 IT Operating Systems Security Policy

12.6 IT Processes and Procedures

12.6.1 Introduction and Objective

Process: A sequence or order of activities that also outlines the different decision points and functions responsible. Processes are cross-functional and define what is done and by whom.

Procedures: Procedures define how certain activities are performed within a process.

12.6.2 Implementation Guidance and Minimum Requirements

Processes are often depicted in diagrammatical form such as a decision tree or flowchart where the work performed is split into logical interrelated steps or “activities”. Processes must always have a “trigger” or start event and a “terminator” or end event that achieves a specific result.

Procedures are typically documented in a step by step order with detailed descriptions of how the work is to be performed and who is responsible for performing the work.

Senqu Municipality must design processes and procedures that are in-line with recognised standards.

The advantage of written processes and procedures will ensure that the Municipality’s outcomes are consistent and repeatable. In addition, written documentation increases the Municipality’s knowledge base.

12.7 IT Organisational Structure

12.7.1 Introduction and Objective

The objectives of establishing an IT organisational structure are as follows:

12.7.1.1 Alignment to new strategic directions of the Municipality.
12.7.1.2 Solve problems resulting from structure inefficiencies.
12.7.1.3 Eliminate job conflicts.
12.7.1.4 Clarify uncertainty regarding the hierarchy and distribution of work and responsibilities.

12.7.2 Implementation Guidance and Minimum Requirements

An internal and external IT organisational structure must be established so that it reflects business needs. In addition, a process must be put in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected Municipal objectives and changing circumstances.

Below are guidelines when designing and reviewing IT organisational structures:

12.7.2.1 Accountability of activities must be placed where ‘means’ and ‘interest’ come together and as low as possible in the IT organisation.
12.7.2.2 The IT organisation structure must be as simple as possible to ensure fast decision-making, improved career planning, simplified IT processes and to prevent bureaucracy and a silo mentality.
12.7.2.3 The IT organisation structure must be appropriate to the size and complexity of the overall Municipality.
12.7.2.4 Unnecessary duplication in functions and job roles must be avoided to ensure uncertainty is not created with regards to roles and responsibilities
12.7.2.5 The IT organisation structure must facilitate knowledge transfer and learning between team members.

The figure below illustrates Senqu Municipality's current IT organisational structure.

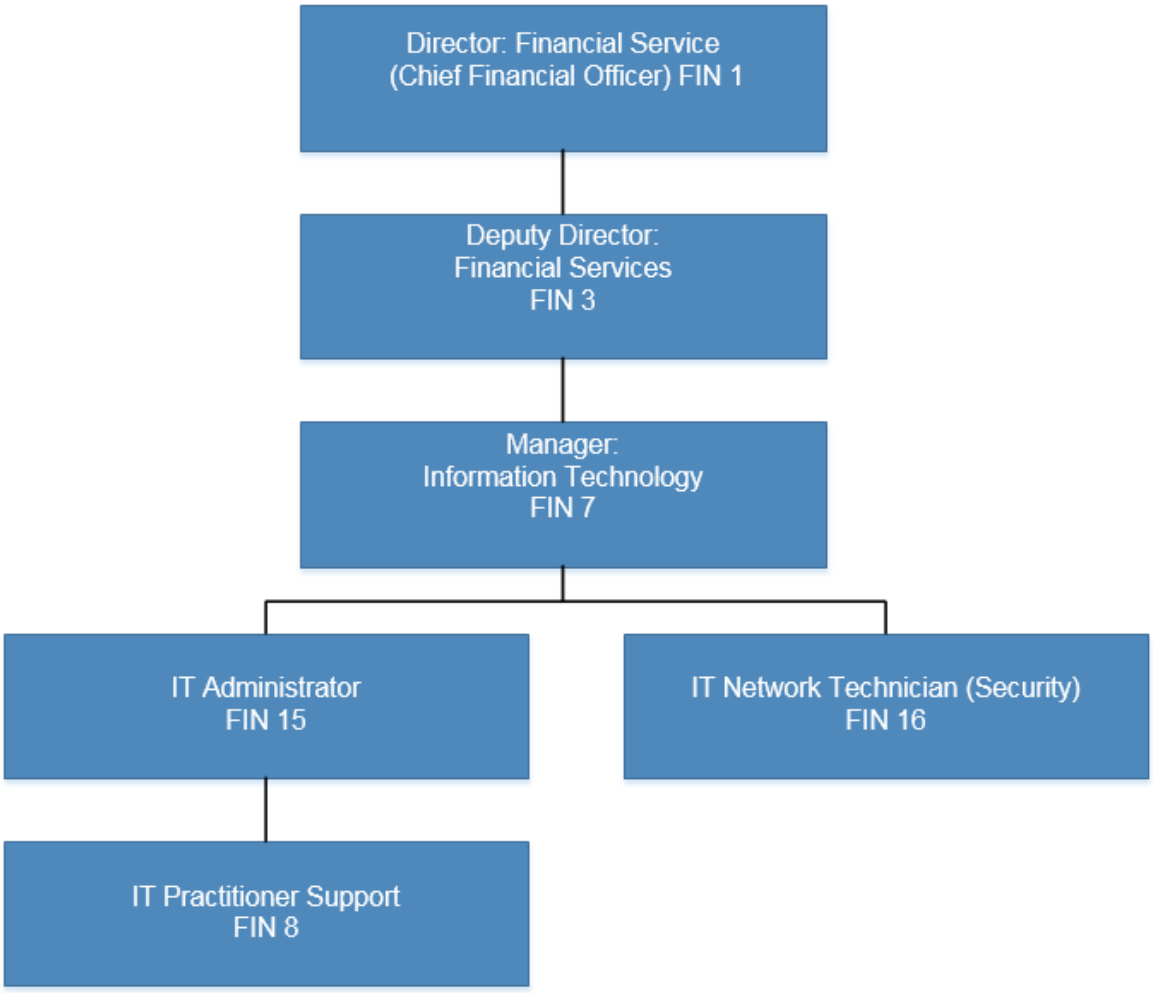

Figure 4: Senqu Municipality's IT Organisational Structure

12.8 IT Job Descriptions and IT Skills

12.8.1 Introduction and Objective

The objective of a job description is to explain the primary role of the position. Job descriptions provide a listing of the specific tasks and duties that the person in the job is responsible for completing. In addition, a job description clarifies the roles and relationships associated with the position.

12.8.2 Implementation Guidance and Minimum Requirements

12.8.2.1 Skills Requirements for Good IT Governance

The following list as described by the South African Local Government Association (SALGA) gives an indication of the type and level of expertise of IT skills that is required to move towards and manage a functional IT Governance Framework.

Table 5: High Level IT Skill Requirements

Skill	General Description
Information Management	The overall management of information, as a fundamental Municipal resource, to ensure that the information needs of the Municipality is met.
Risk Management	The planning and implementation of organisation-wide processes and procedures for the management of operational risk.
Information Security	The management of and provision of expert advice on, the selection, design, justification, implementation and operation of information security controls and management strategies to maintain the confidentiality, integrity, availability, accountability and relevant compliance of information systems.
Security Administration	The authorisation and monitoring of access to IT facilities or infrastructure in accordance with established Municipal policies. Includes the investigation of unauthorised access, compliance with data protection and performance of other administrative duties relating to security management.
Information Assurance	The protection of systems and information in storage, processing, or transit from unauthorised access or modification. Denial of service to unauthorised users; or the provision of service to authorised users.
Systems Architecture	The specification of systems architectures, identifying the components needed to meet the present and future requirements, both functional and non-functional (such as security) of the Municipality as a whole and the interrelationships between these components.
Continuity Management	The provision of service continuity planning and support. This includes the identification of information systems that support critical Municipal processes, the assessment of risks to those systems' availability, integrity and confidentiality and the coordination of

Skill	General Description
	planning, designing, testing and maintenance procedures and contingency plans to address exposures and maintain agreed levels of continuity.
Network Design	The production of network designs and design policies, strategies, architectures and documentation, covering voice, data, text, e-mail, facsimile and image, to support Municipal requirements and strategy.
Network Operations	The day to day operation and maintenance of networked systems to ensure that the communication needs of the Municipality are met.
Programming/Software Development	The design, creation, testing and documenting of new and amended programs from supplied specifications in accordance with agreed standards.
Web Site Specialism	The design, creation, testing, implementation and support of new and amended collections of pages of information on the world wide web or an intranet or extranet.
Project Management	The management of projects, typically (but not exclusively) involving the development and implementation of Municipal processes to meet identified Municipal needs, acquiring and utilising the necessary resources and skills, within agreed parameters of cost, timescales and quality.
Configuration Management	The systematic management of information relating to the documentation, software, hardware and firmware assets of the organisation. This will involve identification and appropriate specification of all configuration items (CIs). Required information will relate to storage, access, problem reporting and change control of CIs.
Change Management	The management of all changes to the components of a live infrastructure, from requests for change (RFC) through to implementation and review, to support the continued availability, effectiveness and safety of the infrastructure.
Capacity Management	The management of the capability and functionality of hardware, software and network components to meet current and predicted needs in a cost-effective manner.
Availability Management	The overall control and management of services and their availability to ensure that all services meet all of their agreed availability targets.
Financial Management for IT	The overall financial management, control and stewardship of the IT assets and resources used in the provision of IT services, ensuring that all governance, legal and regulatory requirements are complied with.
Management and Operations	The management and operation of the IT infrastructure (typically hardware, software and communications) and the resources required to plan for, develop, deliver and support properly engineered IT services and products to meet the needs of a business.

12.9 IT Governance Communication

The communication mechanism that will be used to communicate IT decisions to the various governance structures in place at the Municipality is as follows:

12.9.1 The IT Steering Committee will have a direct communication line the Top Management Committee and will communicate decisions taken in the following domains:

12.9.1.1 IT Governance, Risk and Compliance.
12.9.1.2 IT Strategy.
12.9.1.3 Application Management.
12.9.1.4 Information.
12.9.1.5 Business and IT Architecture.
12.9.1.6 IT Investments and Projects.
12.9.1.7 IT Sourcing.
12.9.1.8 IT Security.
12.9.1.9 IT Operations.
12.9.1.10 General IT Management and Administration.
12.9.1.11 IT Change Management.

12.9.2 The IT Steering Committee will also have an indirect communication line to the Audit and Performance Committee and will communicate decisions taken regarding IT Risk and Compliance.

13. Policy Violations

13.1 Violations of this policy may result in disciplinary action, up to and including dismissal for employees, a termination of employment relations in the case of contractors or consultants, dismissal for interns, or suspension.

14. Policy Review

14.1 This policy is subject to annual review or whenever it is deemed necessary by Senqu Municipality of, to ensure that it is aligned to prevailing resolutions, regulations and market conditions.

15. Publishing the Policy

15.1 The policy shall be made available and accessible to all employees through manuals/hard copies.

16. Senqu Municipality Approval and Sign-Off

Date of Approval by Council: 28 July 2017
Resolution Number: 019/OCM/17

_____ _____

MM YAWA **DATE**
MUNICIPAL MANAGER

RECOMMENDATION

That the report be noted,
That the MCGICT Policy as part of the ICT Corporate Governance Framework be approved by Council.

Appendix A: IT Governance Processes

A1: Management of Exceptions

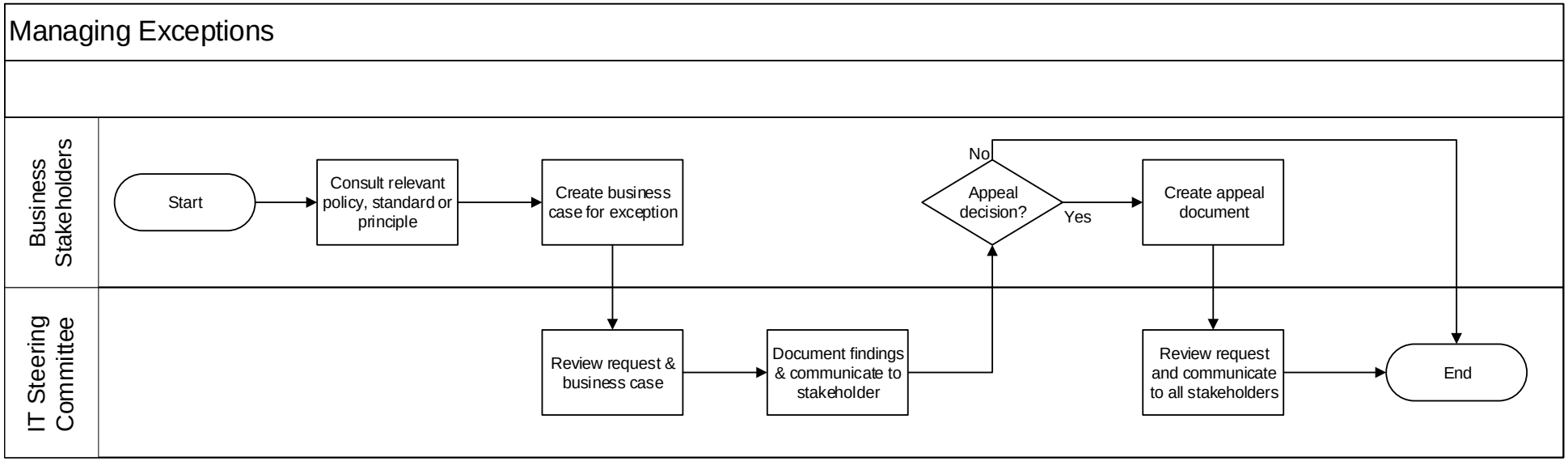

Figure 5: Management of Exceptions

A2: Management of Risk

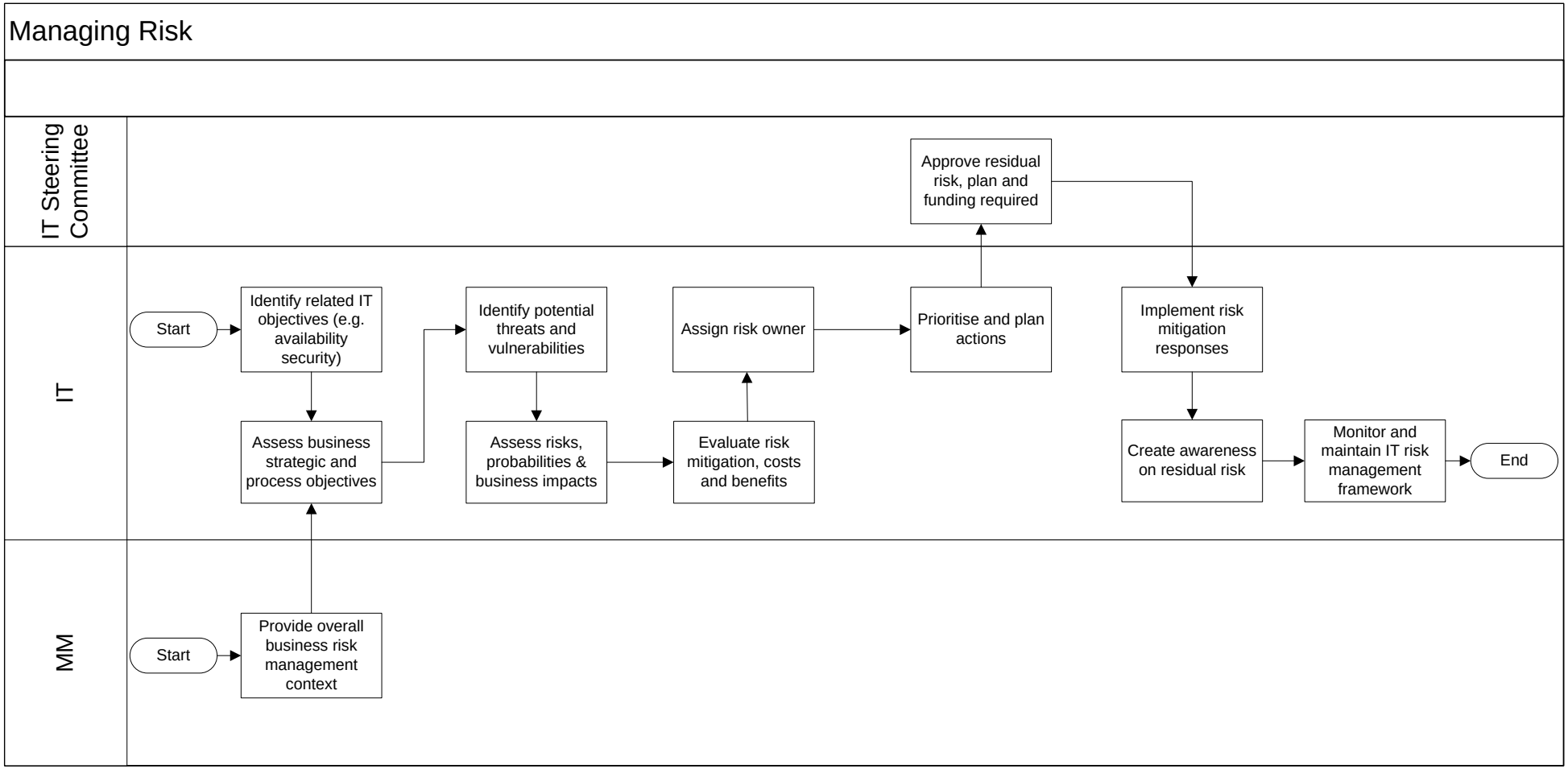

Figure 6: Management of Risk

A3: Agreement and Management of Service Levels

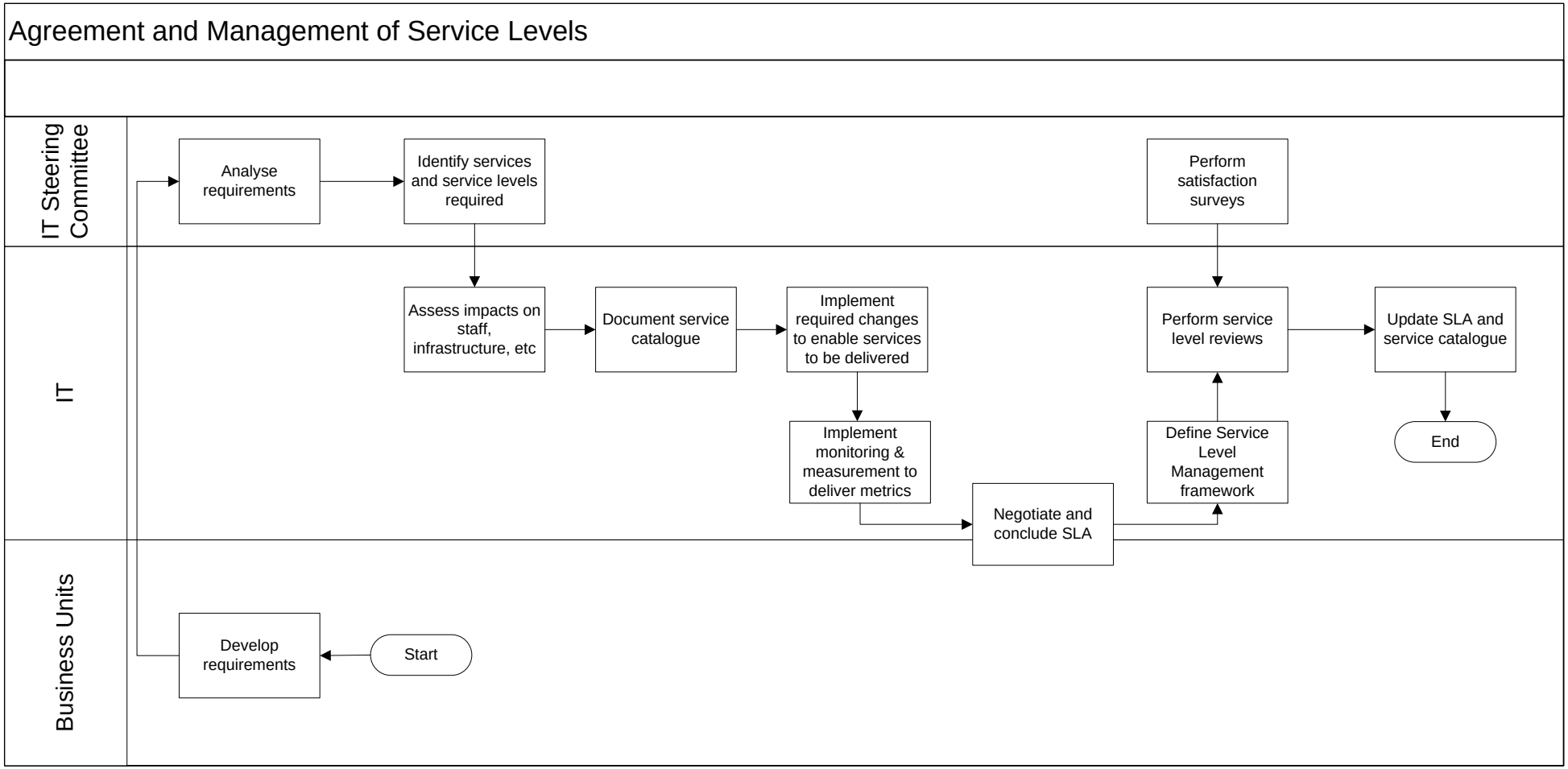

Figure 7: Agreement and Management of Service Levels