INFORMATION &COMMUNICATIONS TECHNOLOGY GOVERNANCE FRAMEWORK FOR MKHAMBATHINI LOCAL MUNICIPALITY

Table of Contents

1. INTRODUCTION 4

- 2. WHAT IS ICT GOVERNANCE? 4
- 3. HOW CAN ICT GOVERNANCE HELP? 5

3.1 ALIGNS ICT WITH INSTITUTIONAL STRATEGY: 5
3.2 INTEGRATES STRUCTURAL REQUIREMENTS: 5
3.3 INTEGRATES BUSINESS AND TECHNOLOGY FOR ICT VALUE: 5
3.4. PROVIDES A MECHANISM FOR UNDERSTANDING THE USE AND OPPORTUNITIES FOR ICT: 5
3.5. IMPROVES BUDGETARY CONTROL AND RETURN ON INVESTMENT: 5
3.6. IMPROVES SELECTION AND USE OF NEW TECHNOLOGIES: 6

- 4. HOW IS ICT GOVERNANCE USED IN THE MUNICIPALITY? 6
- 5. INSTITUTIONAL SYNERGY 7
- 6. GOVERNANCE DECISIONS AND MECHANISMS 7
- 7. ICT GOVERNANCE GUIDELINES 7

7.1 MANAGEMENT OF INFORMATION SECURITY 7
7.2 COMMUNICATION MANAGEMENT 8
7.2.1 WIRELESS 8
7.2.2 BANDWIDTH Parasite 9
7.2.3 MASKING criminal activity 9
7.2.4. FREE access to private data 9
7.3 PROBLEM MANAGEMENT 9
7.4 ASSETS MANAGEMENT 9
7.5 PHYSICAL AND SECURITY CONTROLS 10
7.6 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE 10
7.7 PERSONNEL SECURITY 10
7.8 LOGICAL ACCESS 11
7.9 BUSINESS CONTINUITY MANAGEMENT 11
7.10 MANAGEMENT OF THE THIRD PARTY RELATIONSHIP 11

- 8. GOVERNANCE COMMUNICATIONS AND AWARENESS 12
- **9. GOVERNANCE PERFORMANCE** 12

9.1 Services performance 12
9.2 PERFOMANCE AGAINST INSTITUNAL STRATEGY 12

- 10. ICT DECISION MAKING MATRIX 13

11. ICT GOVERNANCE STRUCTURES AND MODELS 15

- 12. IT PROCESS MODEL 16
- 12. POLICIES TO BE ADOPTED AS PART OF ICT GOVERNANCE 18
- 13. ICT GOVERNANCE STRUCTURES 18

13.1 ICT GOVERNANCE STRUCTURES 18
13.2. ROLES AND RESPONSIBILITIES OF THE ICT GOVERNANCE STRUCTURES 19

- 13.2.1. MANCO 19

13.2.2 DCGITOC 19
13.2.3 ICT STEERING COMMITTEE 19

- 13.2.3.1 ..... LEADERSHIP AND DIRECTION 19
- 13.2.3.2 ..... MONITOR AND EVALUATE 20
- 13.2.3.3 ..... IT REPORTING TO THE MANCO 20

- 14. THE ROLE AND RESPONSIBILITIES: CHIEF INFORMATION OFFICERS 20
- 15. THE ROLE AND RESPONSIBILITY OF A SECURITY OFFICER 22
- 16. INTERNAL AUDIT 23

16.1 ICT INSTITUTIONAL ALIGNMENT 23

1. INTRODUCTION

ICT is one of the key assets of a Municipality. ICT – the people, processes, infrastructure and information - is embedded across the Municipality creating an enterprise wide community of owners and stakeholders. As a major investment ICT is expected to deliver value and has been found to deliver greater 'value' for the Municipality when used as a strategic enabler rather than being influenced by a stream of diverse tactical initiatives.

> A governance structure with buy-in and setting of responsibilities is essential. ... Developing and implementing strategy are not necessarily complimentary. Don't lose sight that strategy means strategy, vision and setting out the direction. ... Responsibility for implementation should be passed on for others to do.

International research revealed that top performing organisations manage their ICT with governance structures that harmonise enterprise objectives and structures with performance goals and metrics. But, although ICT governance is now recognised as the most influential factor in realising 'value' from ICT there is no single model that fits all and each institution will need to develop its own ICT Governance to meet its unique requirements.

> Now consider these key questions:
>
> What is the Municipality's ICT governance structure?

What are your institution's drivers in formulating ICT strategy?

How does the institution manage changes in strategy and exceptions from strategy?

How does the Municipality align institutional strategy and budgets with ICT strategy and budgets?

How does the Municipality assign responsibility and accountability for ICT implementations?

2. WHAT IS ICT GOVERNANCE?

ICT Governance is defines as 'specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT. The complexity and difficulty of explaining IT governance is one of the most serious barriers to improvement.'

ICT governance is about who makes decisions while management is about making and implementing the decisions. Effective ICT governance for the Municipality will answer three questions:

- What decisions must be made
- Who should make these decisions
- How are they made and monitored

3. HOW CAN ICT GOVERNANCE HELP?

Good ICT governance is the foundation for delivering strategic ICT as it:

3.1 Aligns ICT with Institutional strategy:

It provides clear and visible decision making at the appropriate level of senior management, and with ICT embedded across the institution, encourages more responsible and accountable business management, creating focus, understanding and improved delivery against goals. Alignment can deliver cost reductions, improved quality of service delivery, strategies for growth and strategies for diversification

3.2 Integrates structural requirements:

Institutional structures and ICT services are harmonised to allow improved delivery of institutional goals. A less fragmented and more integrated approach to the use of ICT will deliver improved quality of information from the rationalisation and sharing of services

3.3 Integrates business and technology for ICT value:

Involves professionals, research, administration and ICT, resulting in improved decision making and buy-in for ICT changes

3.4. Provides a mechanism for understanding the use and opportunities for ICT:

Improved visibility and accountability for ICT allows institutions to learn from their current ICT experience and encourage improvements for the future. Mechanisms for allowing exceptions to strategy ensure a clear argument; value and justification are visible and understood

3.5. Improves budgetary control and return on investment:

Improved harmonisation between institutional goals and ICT accountability and performance measures improves budgetary control and value. Measures of success are defined as service levels and as evaluation criteria for projects

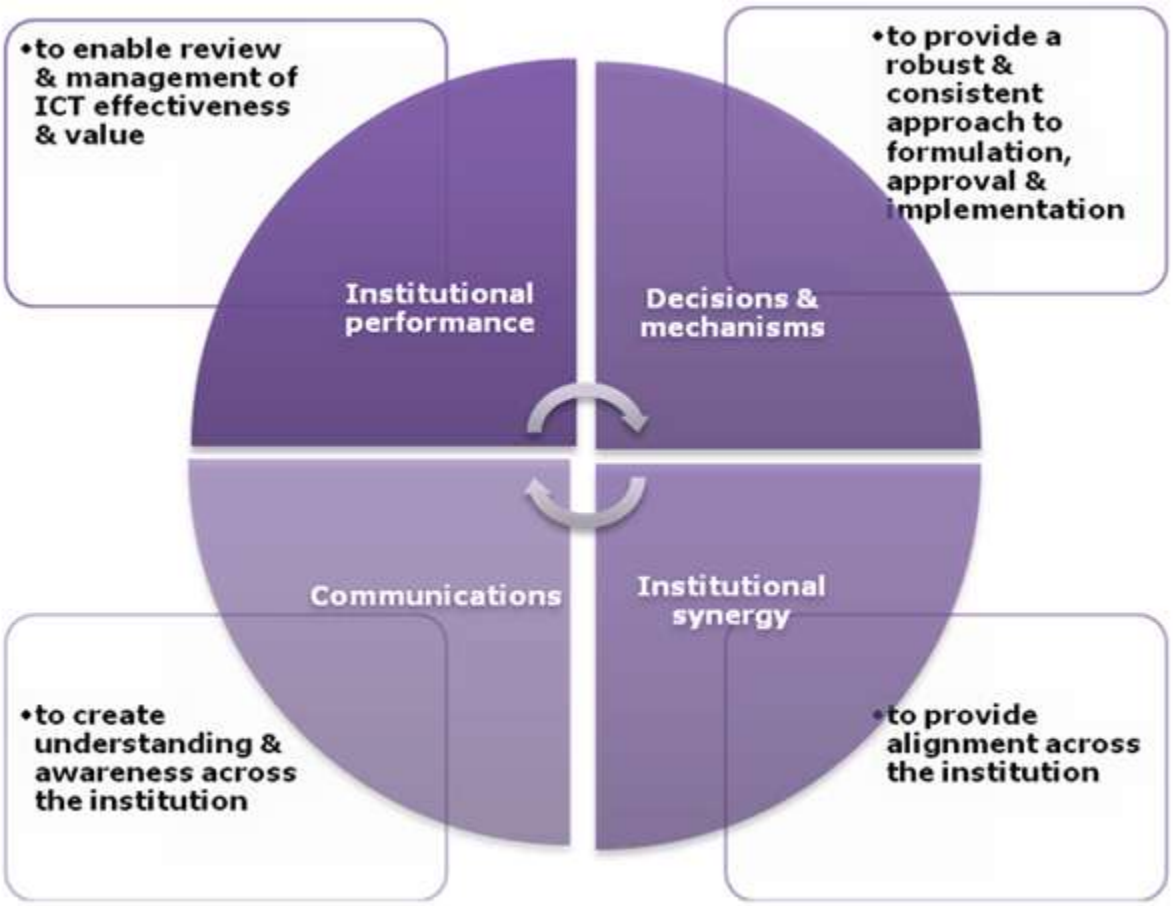
3.6. Improves selection and use of new technologies:

It supports ICT in balancing technological advancement against business priorities and return on investment (ROI)

4. HOW IS ICT GOVERNANCE USED IN THE MUNICIPALITY?

The variations in institutional structures, the different cultures influencing management styles and the ubiquitous nature of ICT within every department leads to wide ranging differences in ICT governance.

However, research findings can be used to highlight the practices that have been found to improve the delivery of strategic ICT. This is presented in these findings across 4 areas as follows:



5. INSTITUTIONAL SYNERGY

The growing importance of ICT in supporting institutional strategy and the need to provide agility requires that an institution is able to have a clear institution-wide view of both current use and future requirements for ICT. Institutions have achieved this by:

- The formulation of a documented and approved Master System Plan (MSP).
- The cross reference of MSP to reinforce alignment to the institutional strategy
- Using a process for review and updating of the strategy

6. GOVERNANCE DECISIONS AND MECHANISMS

In order to ensure that the correct decision are made regarding the deployment of services and systems, the following control mechanism and guidelines shall be put in place :

The ICT steering committee must be established and the post of Chief Information Technology officer must be approved and filled at all times.

The MSP must be approved by the ICT Steering Committee and its implementation must be governed by the ICT steering Committee.

The Information Technology Policy must be approved in accordance with the Municipal policy approval processes and an ICT Security Officer must be appointed to ensure its implementation under the guidance of the Chief Information Technology Officer.

An ICT decision making matrix must be established and used as a guideline for decision making at all level of the Municipality.

All ICT investment must be deliberated and approved by the ICT steering committee and must be in the MSP.

ICT principles, policies and standards must be defined and adhered to. These assist in better decision making and management. It is expected that these will facilitate better investment proposals, progress reporting and measurements for value and ROI and therefore support improved accuracy and availability of information to assist decision making and management

7. ICT GOVERNANCE GUIDELINES

7.1 Management of Information Security

The municipality should ensure that their policy is finalised and approved by the appropriate level of management as a matter of urgency. The policy should then be implemented and communicated formally through a security awareness program. Compliance with the policy should be constantly monitored.

People constitute the greatest risk to any organisation through accidents, mistakes, and lack of knowledge or occasionally through malicious intent. The municipality to make security awareness training compulsory for all to ensure members do not plead ignorance in case of breaches.

The approved policy should be treated as a live document to promote continuous updates if and when changes occur. An individual must be assigned the responsibility for the maintenance of the policy.

7.2 Communication Management

The municipality must have documented standards, procedures or guidelines for the management/administration of their network. Critical system environments must be restricted from the general user environments by implementing virtual private network. Firewalls must be used to inspect traffic passing through the network and the firewall logs are actively monitored and managed in-house.

Intrusion detection system (IDS) and intrusion prevention system (IPS) must be in use. Security systems must be actively monitored and their logs must be not be edited. The municipality was using Trend Micro anti-virus software to detect and prevent electronic viruses.

The municipality must have patch management framework in place. Meaning that their systems were vulnerable to compromises. If the municipality allows wireless access it was must be appropriately controlled or/and managed.

Dealing with an information breach is not only embarrassing but also has legal implications since there are notification requirements if sensitive employee or customer data is accessed inappropriately or potentially exposed to a breach. The development of a patch management strategy is therefore critical for the Municipality to:

- determine the methods of obtaining patches
- specify methods of validating patches
- identify vulnerabilities that are applicable to the organisation
- ensure all patches are tested against known criteria describes a detailed deployment method for patches
- report on the status of patches deployed across the organisation
- includes methods of dealing with patch failures

7.2.1 Wireless

Wireless is a great technology that offers many benefits and requires great responsibility. A responsibility that is unfortunately much too often ignored when implementing it. A wireless network needs to be properly secured as it poses a number of extremely serious risks and dangers if left wide open and exposed, which many users are unaware of such as:

7.2.2 BANDWIDTH PARASITE

Where the intruders uses the victim's broadband connection to get online without paying. This will not cause any direct harm to the compromised network, but it can slow down internet or network access for the victim

7.2.3 MASKING CRIMINAL ACTIVITY

Where an unauthorized user could abuse the victim's connection for malicious purposes like hacking, launching a DOS attack, or distributing illegal material.

7.2.4. FREE ACCESS TO PRIVATE DATA

A wireless network is also a direct backdoor into the victim's private network – literally. Instead of intruding from the public side of the gateway device, the intruder connects directly to the network on the private side of the gateway device, completely bypassing any hardware firewall between the private network and the broadband modem. The intruder can completely take advantage of this by snooping around undisturbed and getting access to confidential data.

It is therefore imperative that uMgungundlovu municipality should develop policies and procedures that will govern the security of their wireless

7.3 Problem Management

The municipality must have operational procedures for the management of faults/incidents in the use or implementation of ICT services that users, third parties and contractors were aware of. It must also indicate that the documented procedures must address planning and preparation, detection, initiation, evaluation containment, eradication, response, recovery, closure post-incident.

Incidents must be tracked to identify trends and underlying causes of operational failures with the view to long term solutions.

The municipality need to have emergency response process for dealing with serious incidents. The process includes:

- definition of an emergency situation or incident
- detailed description of roles and responsibilities
- defined response process allowing critical decision to be made quickly
- defined steps to be taken in emergency situations
- contact details for all key personnel

The municipality should enforce good practices in the management of problems/incidents. Management should ensure that they harmonise the discord that currently exist between procedures and processes.

7.4 Assets Management

The municipalities must have internal controls over the management of information assets appeared satisfactory. The municipality must keep an asset register, which requisite to be updated regularly as

and when changes occur. The asset register held important information about each asset such as asset owner, asset location, and date of acquisition.

The municipality should protect the asset register from unauthorised changes by limiting access rights.

7.5 Physical and Security Controls

To minimise the risks of unauthorised physical access to premises and sensitive areas, the municipality should manned reception where visitors need to sign-in with the security guards, burglar doors, CCTVs and access cards. Visitors must record their name, time of entry and the person being visited. Authorisation need to be required before ICT equipment could be taken outside the municipal premises and a register of all equipment taken offsite and returned must be kept. The server room must be equipped with an air conditioner, UPS, smoke detectors, fire suppression system and raised floors to protect it from environmental hazards such as flooding, fire and power outages.

The municipality should continue enforcing good practices with regard to physical security and environment controls.

7.6 System Acquisition, Development and Maintenance

The municipality should consider developing change control procedures manage their change control procedures that will ensure only authorised system and/or infrastructure changes are introduced to the production environment. The procedures should cover:

- identification and recording of significant changes (formal change request form)
- formal approval procedure for proposed changes (change control committee)
- restricting access to program source to authorised personnel (segregating developers/database administrator/user responsibilities)
- planning and testing of changes prior implementation (unit testing, interface, user testing, full functionality testing, etc)
- assessment of potential security impacts
- communication of change details to all relevant persons
- procedures for emergency changes
- formulation of a back-out plan(s) prior to effecting a change(s)
- importantly that all system software and hardware development and maintenance be subjected to quality assurance review

7.7 Personnel Security

The municipality must conduct the personnel security management process. The entity's personnel management process must include the following:

- Background screening of staff

- Signing of confidential statements and conditions of employment
- Termination procedures
- Background screening of contractors and third parties
- Development of job descriptions/job profiles for employees
- Security clearance by NIA for security personnel

The Municipality should follow best practises that will ensure that competent and a security conscious personnel is appointed.

7.8 LOGICAL ACCESS

The municipality need to documented user account management procedures that cover user access at both network and application system level. The procedures need to include the following:

- Process for requesting new user access and allocating access rights
- Segregation of access control role
- Process for modifying user privileges
- Process for terminating existing access
- Regular checks of administrator activities

Municipality must enforce good practices and researching new ways of improving security within their organisation. The municipality should make sure that sign-on mechanism is tighten security by making sure the system administrators are forced to use different logging credential when performing their administrator functions and normal user responsibilities. The activities of administrators should be closely monitored to ensure that the rights are not used for unauthorised acts.

7.9 BUSINESS CONTINUITY MANAGEMENT

The security management of the Municipality should ensure that the information risk assessment is conducted to inform the municipality's business continuity plan and the ICT disaster recovery plan.

- The starting point should be an understanding of critical business process,
- Followed by the identification and an inventory of the information assets that support these processes.
- Thirdly, identification of possible security threats against each asset and the impact it might have on business.
- Lastly, the municipality should put together a control mechanism that will minimise the impact of the threat should it materialise.

7.10 MANAGEMENT OF THE THIRD PARTY RELATIONSHIP

If the municipality has Outsource IT functions and the outsource relationships must be managed by a contract agreement. Contracts contain appropriate clauses with respect to:

- adherence to corporate security
- adherence to internal control policies and standards for information technology and,
- penalties in cases of non-compliance

The municipality has also developed a process for managing third party service delivery that entails:

- regular service reports by the service provider
- service level meetings with the service provider and,
- assigning the responsibility for service monitoring to a specific individual

The municipality should enforce good practices in the management of their third party relationships.

8. GOVERNANCE COMMUNICATIONS AND AWARENESS

Communications have always been accepted as key to the successful delivery of ICT projects. However, the ability to address and balance the priorities within strategic planning intensifies the need for communications between institutional management. In addition to consultation on strategic requirements there are other techniques that have been found to enhance institutional awareness and buy-in to strategy:

- Obtain MANCO buy-in and promotion of ICT governance.
- Use Committees across the municipality to add awareness and create influence.
- Use a Security Officer and a compliance function to own and promote ICT governance.
- Identify and try to win over management who don't comply.
- Provide a portal (intranet) to use for promoting ICT governance information to ease its use and assist in visibility.

9. GOVERNANCE PERFORMANCE

Governance allows for the measurement of performance in two areas:

9.1 SERVICES PERFORMANCE

Definitions for ICT service levels, and project progress reporting provide both project and operational management and reporting to the ICT steering Committee. Service levels defined and agreed as part of the ICT governance must be actively used for service communications and monitoring. A tool must be developed in order to improve reporting in relation to project progress and final delivery against objectives

9.2 PERFOMANCE AGAINST INSTITUNAL STRATEGY

Each Head of Department must gauge how well ICT governance is delivering ICT services that meet the core institutional strategic objectives.

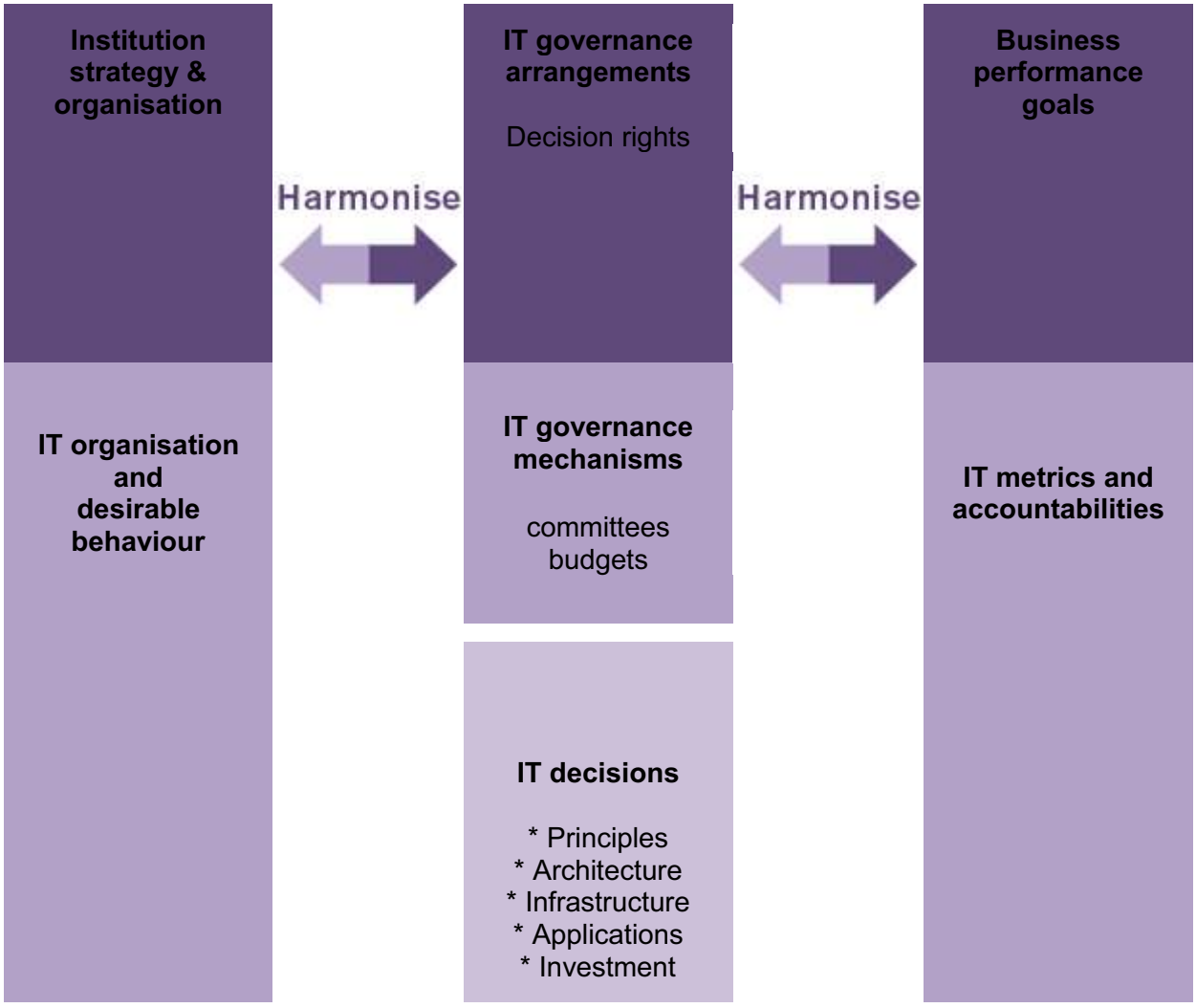
The assessment requires:

1. The definition of a set of strategic objectives or outcomes. For example cost effectiveness, transformation, business improvement or agility
2. each member of the management team to assess for their domain
    a. the importance of each of the outcomes
    b. the influence of governance on the success of each of the outcomes
    c. where and why is governance effective
    d. where and why is governance less effective?

10. ICT DECISION MAKING MATRIX

They state that ICT governance is about who makes decisions while management is about making and implementing the decisions. They assert that effective ICT governance will answer three questions:

- What decisions must be made
- Who should make these decisions
- How are they made and monitored



The above framework diagram illustrates the requirement for harmonisation of institutional strategy and organisation with ICT governance arrangements and the institutional performance goals.

The institutional strategy, ICT governance arrangements and performance goals are enacted through the ICT organisation and desirable behaviours, ICT governance mechanisms and performance metrics, respectively.

The adopted ICT governance methodology suggest that there are five interrelated ICT decisions that should be considered together with the decision making structure and the following diagrams have been adapted from their work to illustrate a governance framework:

<table>
<tr><th colspan="3">Key ICT Governance Decisions</th></tr>
<tr><td colspan="3">1 ICT principles
High-level statements about how ICT is to be used in the institution</td></tr>
<tr><td rowspan="2">2 ICT architecture decisions

Organising logic for data, applications, and infrastructure

These are captured in a set of policies, relationships and technical definitions

They ensure the desired institution and technical standards and levels of integration are achieved</td><td>3 ICT infrastructure decisions

Centrally co-ordinated, shared ICT services that provide the foundation for the enterprise’s ICT capability</td><td rowspan="2">5 ICT investment and prioritisation decisions

Decisions about how much and where to invest in IT, including project approvals and justification techniques</td></tr>
<tr><td>4 Institutional applications needs

Specifying the institutional need for purchased or internally developed ICT applications</td></tr>
</table>

The institution is required to decide the governance arrangements for each key decision area. The harmonising of each decision making group will significantly affects the decisions and outcomes and is therefore able to effect strategy alignment. The groups or governance archetypes have been categorised as:

CODE	*Name*	*Description*
IT001	*Institutional monarchy*	*Municipal Manager and Heads of Department*
IT002	*ICT monarchy*	*ICT Steering Committee*
IT003	*User Forum*	*User Forum representing users from each Department*
IT004	*System Owners*	*System owners and vendors (hardware and software) of technologies used in the Municipality.*
IT005	*Super Users*	*Isolated individual or small decision group*

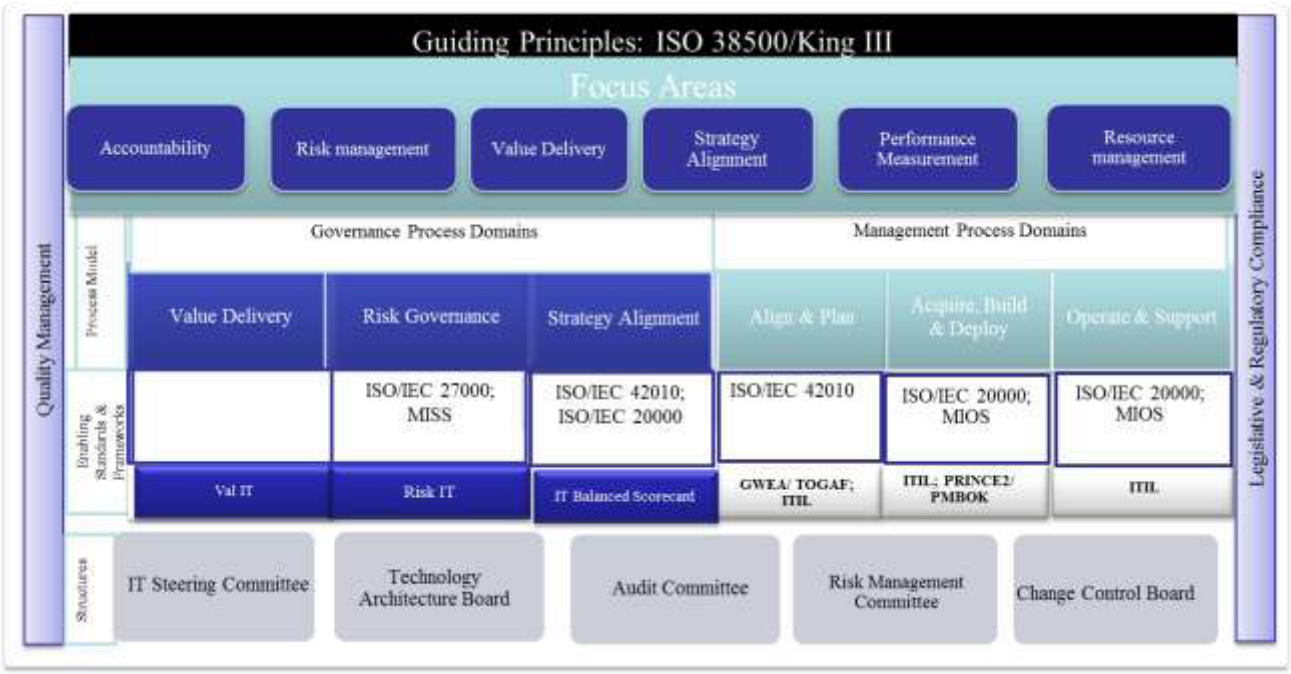
IT006	*Technology Specialist*	*Service Providers, Specialists, Vendors*

These archetypes are used below to illustrate an example governance structure:

An example of the ICT governance decision making structure									
ICT Principles		ICT Architecture		ICT Infrastructure Strategies		Institutional Application needs		ICT Investment	
input	decision	input	decision	input	decision	input	decision	input	decision
IT003	IT002	IT005	IT002	IT005	IT002	IT004	IT002	IT002	IT001
IT004		IT004		IT004		IT005	IT001		
		IT006		IT006					

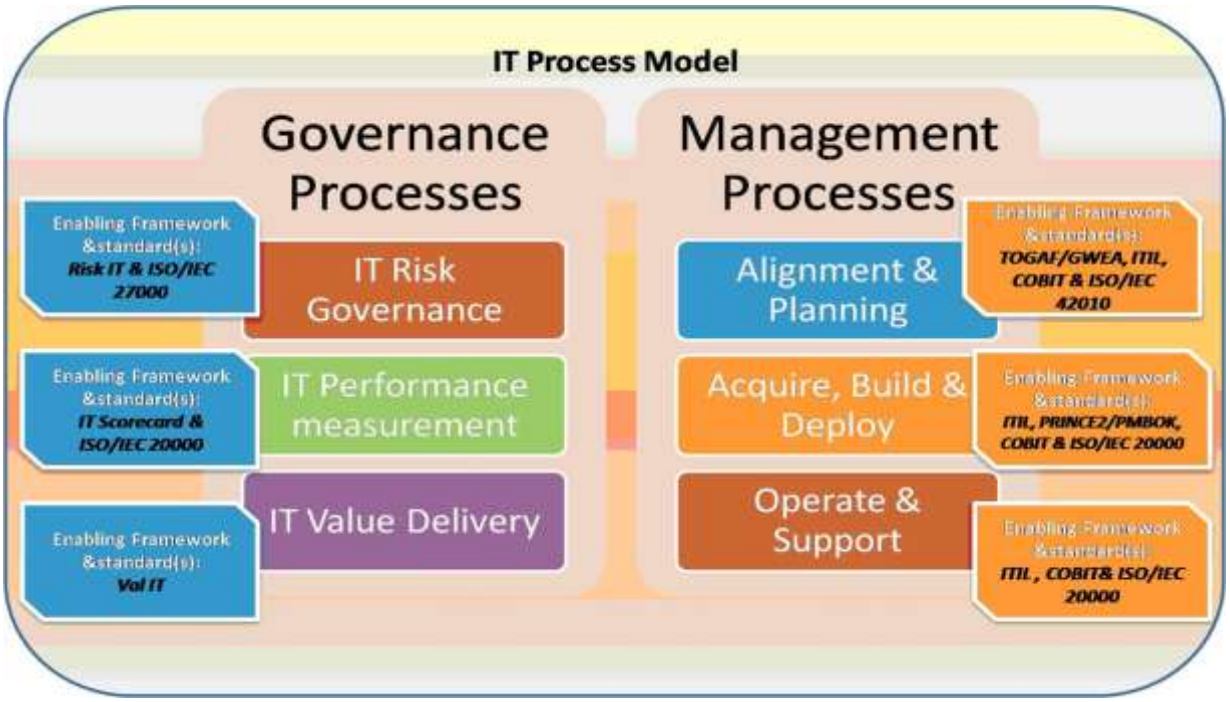
11. ICT GOVERNANCE STRUCTURES AND MODELS

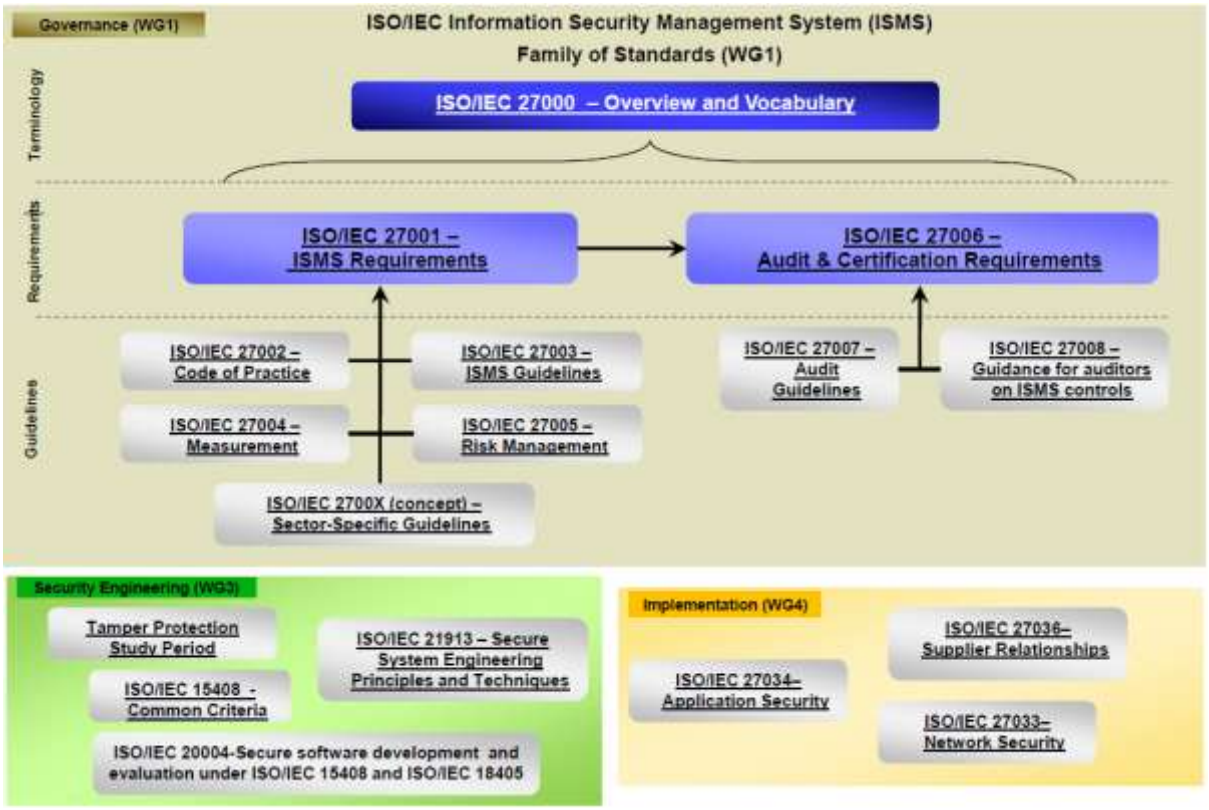
Guiding Principles for ICT

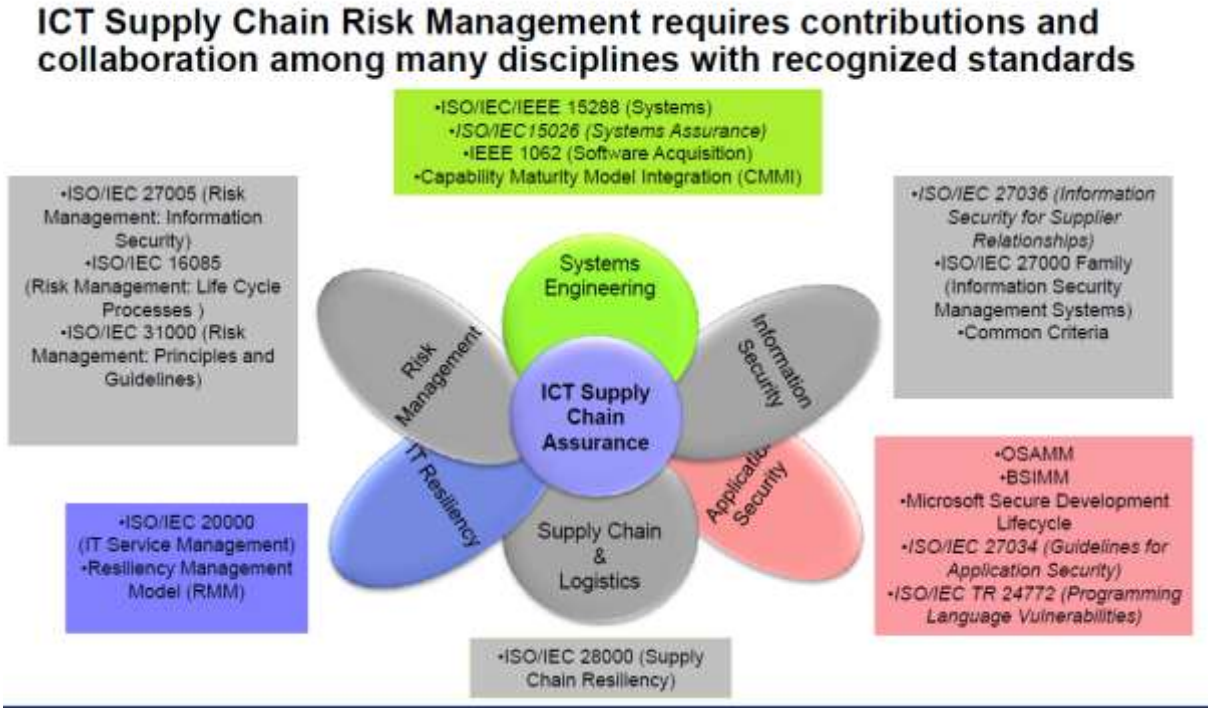


The above diagram depicts all the adopted national and international standards and guidelines for the Municipalities ICt governance framework. All the above shall be used in formulating policies, rolling out projects and in deploying and controlling ICT services.

12. IT PROCESS MODEL




Governance (WG1)
ISO/IEC Information Security Management System (ISMS)
Family of Standards (WG1)
Terminology
ISO/IEC 27000 – Overview and Vocabulary
Requirements
ISO/IEC 27001 – ISMS Requirements
ISO/IEC 27006 – Audit & Certification Requirements
Guidelines
ISO/IEC 27002 – Code of Practice
ISO/IEC 27003 – ISMS Guidelines
ISO/IEC 27004 – Measurement
ISO/IEC 27005 – Risk Management
ISO/IEC 2700X (concept) – Sector-Specific Guidelines
ISO/IEC 27007 – Audit Guidelines
ISO/IEC 27008 – Guidance for auditors on ISMS controls
Security Engineering (WG3)
Tamper Protection Study Period
ISO/IEC 21913 – Secure System Engineering Principles and Techniques
ISO/IEC 15408 - Common Criteria
ISO/IEC 20004-Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405
Implementation (WG4)
ISO/IEC 27036– Supplier Relationships
ISO/IEC 27034– Application Security
ISO/IEC 27033– Network Security


ICT Supply Chain Risk Management requires contributions and collaboration among many disciplines with recognized standards
•ISO/IEC/IEEE 15288 (Systems)
•ISO/IEC15026 (Systems Assurance)
•IEEE 1062 (Software Acquisition)
•Capability Maturity Model Integration (CMMI)
•ISO/IEC 27005 (Risk Management: Information Security)
•ISO/IEC 16085 (Risk Management: Life Cycle Processes)
•ISO/IEC 31000 (Risk Management: Principles and Guidelines)
•ISO/IEC 27036 (Information Security for Supplier Relationships)
•ISO/IEC 27000 Family (Information Security Management Systems)
•Common Criteria
Systems Engineering
Risk Management
Information Security
ICT Supply Chain Assurance
IT Resiliency
Application Security
Supply Chain & Logistics
•ISO/IEC 20000 (IT Service Management)
•Resiliency Management Model (RMM)
•OSAMM
•BSIMM
•Microsoft Secure Development Lifecycle
•ISO/IEC 27034 (Guidelines for Application Security)
•ISO/IEC TR 24772 (Programming Language Vulnerabilities)
•ISO/IEC 28000 (Supply Chain Resiliency)

12. POLICIES TO BE ADOPTED AS PART OF ICT GOVERNANCE

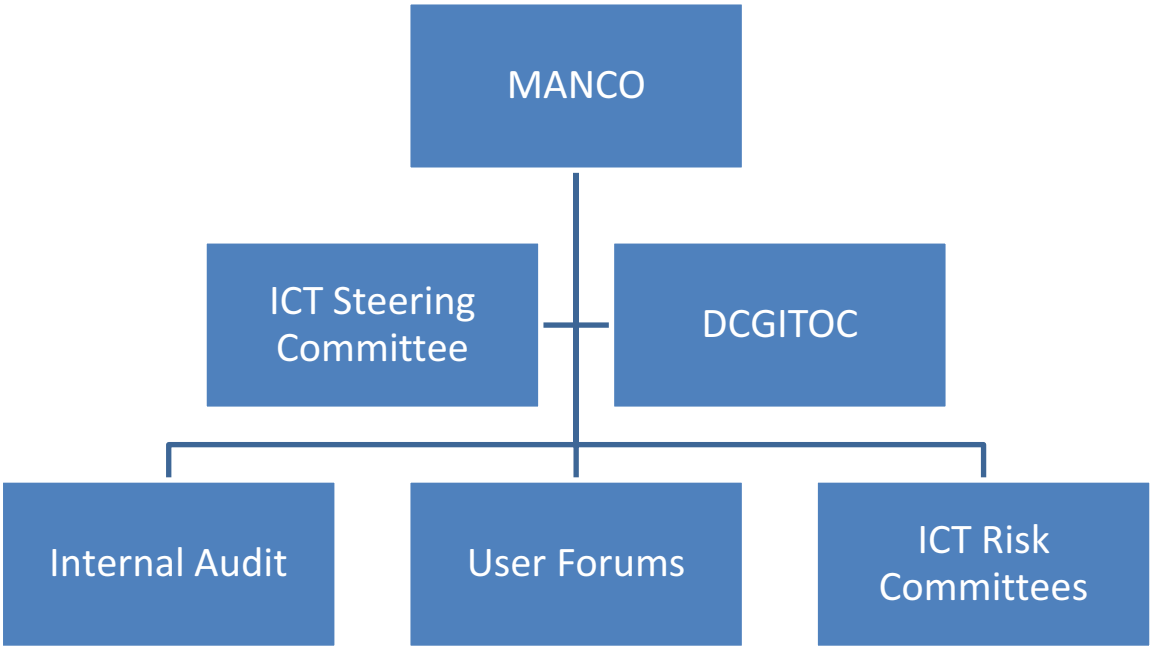
A consolidated Information & Communication Technology usage and Security Policy will be developed and adopted by the Municipality. The Policy shall be guided by the following:

1. INFORMATION SYSTEMS SECURITY POLICY
2. INTERNET USAGE POLICY
3. EMAIL USAGE POLICY
4. Network Usage Policy
5. Front End Peripheral Usage Policy
6. Physical Access and Environmental Control Policy
7. Logical Access Control Policy
8. Antivirus and Software Updates Policy
9. Backup and Restore Policy
10. Network Management & Procedure Policy

13. ICT GOVERNANCE STRUCTURES

13.1 ICT Governance Structures

The following organogram depicts the ICT governance structures for the Municipality.



13.2. Roles and Responsibilities of the ICT Governance Structures

13.2.1. MANCO

MANCO must play an oversight role on ICT projects and activities and must also ensure that ICT is budgeted for in their respective departments.

13.2.2 DCGITOC

The District Government Information Technology Council shall facilitate co-ordination and sharing of ICT services between the Municipality and other role players.

13.2.3 ICT STEERING COMMITTEE

The ICT Steering Committee must be responsible for the following:

13.2.3.1 LEADERSHIP AND DIRECTION

Articulate the Municipality's goals and vision, drive, guide and inspire. It must direct Municipality's strategies and operations with a view to achieving sustainable economic, social and environmental performance.

The Committee is to:

- Place IT on the board agenda
- Clarify business strategies and objectives, and the role of IT in achieving them

- Delegate responsibility for implementing an IT governance framework
- Determine and communicate levels of risk tolerance/appetite
- Assign accountability for the organisational changes needed for IT to succeed.

13.2.3.2 MONITOR AND EVALUATE

The Committee is to:

- Ensure that IT is aligned with Municipality's objectives.
- Monitor and evaluate the extent to which IT actually sustains and enhances the company objectives.
- Monitor and evaluate the acquisition and appropriate use of technology, process and people
- Ensure that an internal control framework has been adopted, implemented and is effective
- Use the risk and audit committees to assist the board fulfil its responsibilities
- Obtain project assurance from independent experts that IT management apply all basic elements of appropriate project management principles to all IT projects.
- Obtain independent assurance of the governance and controls supporting outsourced services.
- Monitor the application of King III governance principles by all parties, at all levels (starting with the Committee), at all stages of business operations, across organisational boundaries (including third parties) and for the acquisition and disposal of IT goods and services.

13.2.3.3 IT REPORTING TO THE MANCO

Management should increase transparency and provide the board with complete, timely, relevant, accurate and accessible information about:

- The likelihood of IT achieving its objectives?
- IT's resilience to learn and adapt?
- The judicious management of the inherent risks from using IT, including disaster recovery?
- How well IT has recognised opportunities and acted on them?

The Committee should take steps to ensure that resources are in place to ensure that comprehensive IT reporting is in place, both to the board by management and by the board in the integrated report.

14. THE ROLE AND RESPONSIBILITIES: CHIEF INFORMATION OFFICERS

The Municipality is to appoint a suitably qualified and experienced individual as the chief information officer who is expected to:

- Interact regularly on matters of IT governance with the board, or appropriate board committee, or both understand the accountability and responsibility of IT.
- Implement an IT Governance framework to deliver value and manage risk.

- Implement an Accountability framework to assign decision-making rights.
- Implement a suitable organisational structure and define terms of reference.
- Incorporate IT into the business processes in a secure, sustainable manner.
- Implement an ethical IT governance and management culture
- Implement an IT control framework
- Obtain assurance on the effectiveness of the IT control framework
- Implement processes to ensure that reporting to the board is complete, timely, relevant, accurate and accessible
- Implement a strategic IT planning process that is integrated with the business strategy development process.
- Integrate IT plans with the business plans
- Define, maintain and validate the IT value proposition
- Align IT activities with environmental sustainability objectives
- Include relevant representation from the business in oversight structures
- Have regard for the legislative requirements that apply to IT
- Translate business requirements into efficient and effective IT solutions
- Support the business and governance requirements in a timely and accurate manner through the acquisition of people, process and technology
- Optimise resources usage, leverage knowledge
- Ensure that the business value proposition is proportional to the level of investment
- Deliver the expected return from IT investments
- Protect information and intellectual property
- Promote sharing and re-use of IT assets
- Monitor and enforce good governance principles across all parties in the chain from supply to disposal of IT services and goods
- Obtain independent assurance that outsourced service providers have applied the principles of IT governance
- Obtain independent assurance of the effectiveness of the IT controls framework implemented by service providers
- Obtain independent assurance that the basic elements of appropriate project management principles are applied to all IT projects
- Regularly demonstrate to the board that the company has adequate business resilience arrangements in the event of a disaster affecting IT
- Implement a risk management process based on the boards risk appetite
- Select and use an appropriate framework for managing risk (e.g. COSO)
- Comply with applicable laws and regulations
- Implement an IT controls framework
- Manage information assets effectively
- Implement an information security management system in accordance with an appropriate
- information security framework
- Provide the Audit and Risk Committees with relevant information about IT risks and the controls in place
- Measure, manage and communicate IT performance
- Report to the IT Steering Committee on IT performance.

15. THE ROLE AND RESPONSIBILITY OF A SECURITY OFFICER

The Municipality must appoint a Security Officer who will support the head of the institution or the CITO by performing the formally delegated responsibilities in respect of IT security. The head of the institution should formally delegate these responsibilities to the security officer, which should at least include the following:

- Develop and maintain an IT security policy, as well as security procedures and standards for the operating unit and provide guidance consistent with the municipality's requirements and the specifications of the MISS.
- Conduct reviews of all systems to ensure that effective IT security policies are in place for each system and include the following:
    - Risk assessments
    - Current and effective IT security plans that are integrated into all stages of the system life cycle
    - Annual system assessments
    - Current and tested contingency plans
    - Current certification and accreditation
- Conduct annual assessments of the operating unit's IT security programme to confirm the effective implementation of and compliance with established policies and procedures.
- Establish a process for tracking remedial actions to mitigate risks in accordance with the institution's standard for plans of action and milestones.
- Maintain the IT system inventory in accordance with the institution's standard for inventory management.
- Establish a process for ensuring that all users (such as the IT security officer, system administrators, contracted staff, technical representatives) are periodically briefed about IT security awareness and receive copies of rules of behaviour, as well as training to enable them to fulfil their IT security responsibilities and understand the consequences of non-compliance.
- Act as the operating unit's central point of contact for all incidents, develop procedures for dealing with incidents and report all incidents to the incident response function.
- Participate as a voting member in the institution's IT security coordinating committee (SCC), as well as in special committees under the IT SCC and provide other support to the IT SCC as required.
- Cooperate with the institution's accounting officers and the CIO on IT security matters (concerning incidents, potential threats and other concerns).
- Ensure that system owners establish processes to ensure that:
    - IT personnel receive specialised training

- access privileges are revoked in a timely manner (e.g. after transfer, resignation, retirement, change of job description, etc.). In the case of individuals who are separated for adverse reasons, such privileges should be revoked immediately upon, or just prior to notification of the impending action.

- Serve as certification agent for systems within his/her operating unit (except in the case of systems for which the IT security officer is also the system owner, or moderate and high-impact systems for which the IT security officer is also the IS security officer).
- Establish a process for identifying, tracking and reporting on security patch management.
- Establish a chain of custody that documents the name, title, office and telephone number of each individual who has sequential possession of a system's hard drive when it is removed due to compromise and might be subjected to forensic examination as evidence in potential prosecutions.
- Ensure that cryptography is used for the transmission of classified information that impacts national security, in accordance with the institution's security policy.
- Ensure that IT security is addressed in the development and acquisition of information systems and security-related products and services by:
    - following a methodology for security considerations in the information system development life cycle
    - working with system owners to determine the information type and system impact levels and the control baseline for the protection of the system and its data
    - working with system owners to ensure the integration of the system security configuration into the security architecture, which, in turn, is integrated into the institution's overarching IT enterprise architecture.
- Ensure that network and system warning banners communicate that there is no expectation of privacy in the authorised or unauthorised use of IT systems.
- Ensure that the institution's policies and practices allow for the following account management controls:
    - Creation of accounts based on formal requests and authorisation by the users' supervisors
    - Identification and documentation of user accounts with appropriate access levels/account permissions
    - Account termination
    - Periodic status reviews of all currently open accounts on all systems through the auditing (review) of user accounts (employee, contractor and guest accounts)
- Administer access control software.
- Review access rights on a regular basis to ensure compliance with the data security policies and procedures.

Monitor security and investigate security violation attempts.

16. INTERNAL AUDIT

16.1 ICT Institutional Alignment

ICT must be taken as a strategic support function of the Municipality and should be located under the office of the Municipal Manager as recommend by the King III report on corporate governance.