



Information Communication Technology (ICT) Strategic Plan

Business Areas	Economic, Social and Integrated Development Services
Operational Area	ICT Department
Version	01.19
Review Date	March 2026
File Name	ICT Strategic Plan
Business Owner	Manager ICT
Approved by	Council
Date Approved	31 March 2026

Table of Contents

Definitions & Acronyms	2
1 PURPOSE	3
2 STRATEGIC ICT PLAN APPROACH.....	4
3 ORGANISATIONAL STRUCTURE.....	7
4 LINKING STRATEGIC DIRECTION	7
5 ICT STRUCTURE.....	15
6 LIST OF CURRENT APPLICATIONS / SYSTEMS IN USE.....	15
7 GAP ANALYSIS	15
8 ICT LIFECYCLE.....	16
9 Business Continuity Management.....	16
10 ICT Governance Framework Decision Making Process.....	17
10.1 Decision Rights	19
10.2 Resource requirements and services	21
10.3 Roles and Responsibility Categories	21
10.4 Vision, Planning and Operations Governance	21
10.5 Defined Processes.....	23
10.6 The Business Continuity Committee.....	24
10.7 Business Continuity Committee Responsibilities.....	24
10.8 Business Continuity Committee Membership.....	25
10.9 Frequency and Scheduling of Meetings.....	25
11 Reference List	26
12 Endorsement	27
13 Document History	28

Definitions & Acronyms

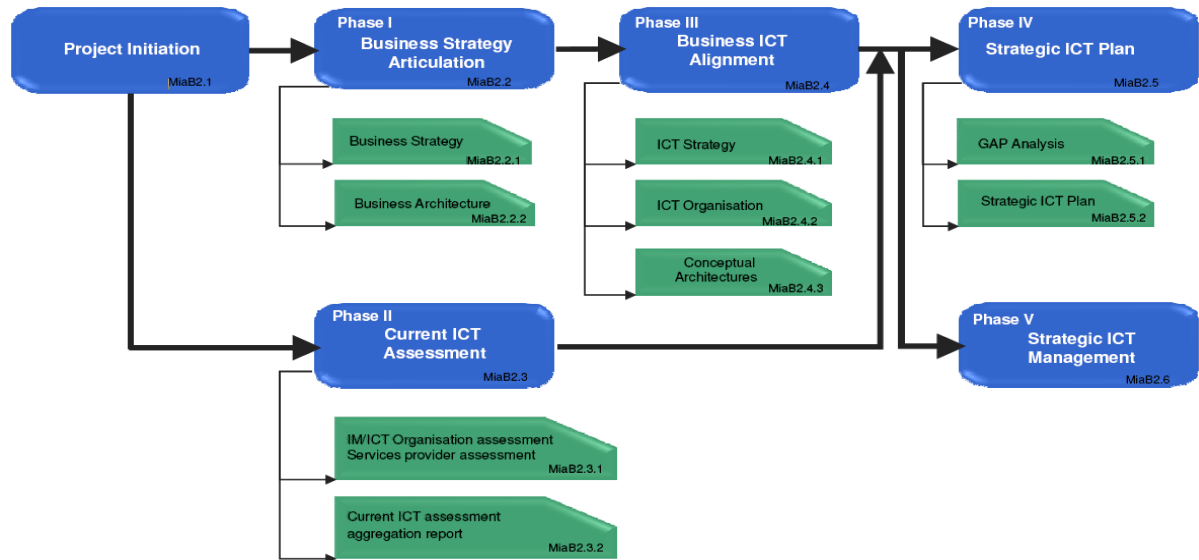
Application	Computer software that causes a computer to perform useful tasks
MM	Municipal Manager
CIO	Chief Information Officer
Hardware	The component devices that are the building blocks of computers
ICT	Information, Communication, and Technology
IDP	Integrated Development Plan
ISACA	Information Systems Audit and Control Association
KPA	Key Performance Areas
KPI	Key Performance Indicator
MFVM	Municipal Financial Viability and Management
Network	A telecommunications network that connects a collection of computers to allow communication and data exchange between systems, software applications, and users
SALGA	South African Local Government Agency
SMT	Strategic Management Team

1 PURPOSE

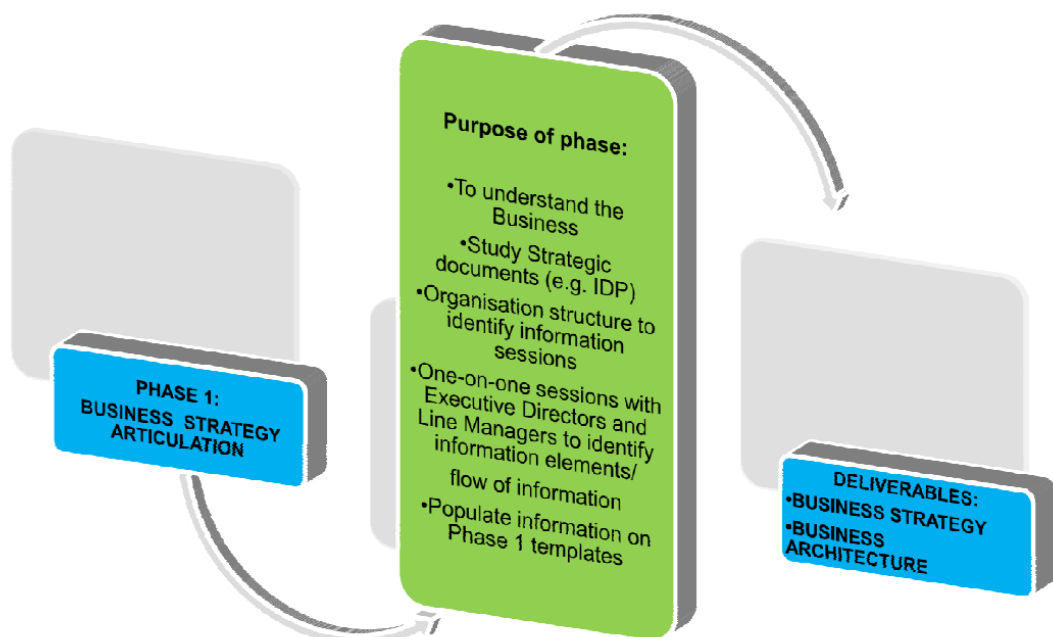
To provide an overall summary on specific outputs of the Municipal ICT Strategy Plan (MICTSP) for the Langeberg Municipality. This document ensures the alignment of the Municipality IDP with the ICT Objectives through a streamlined and governable process. The MICTSP is thus existing in tandem to the IDP and should reviewed in accordance with the IDP review processes.

2 STRATEGIC ICT PLAN APPROACH

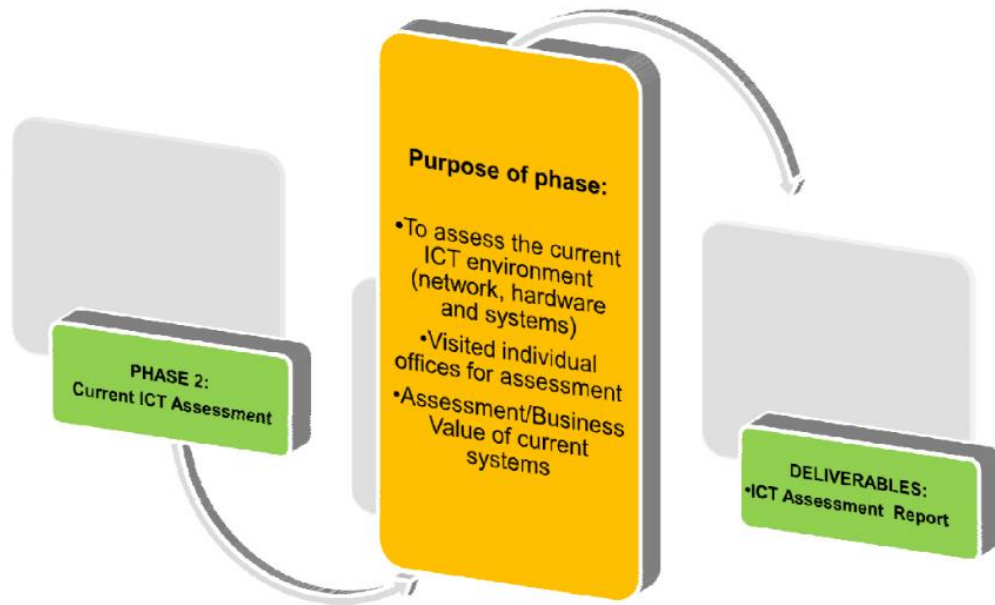
Strategic ICT Planning Framework



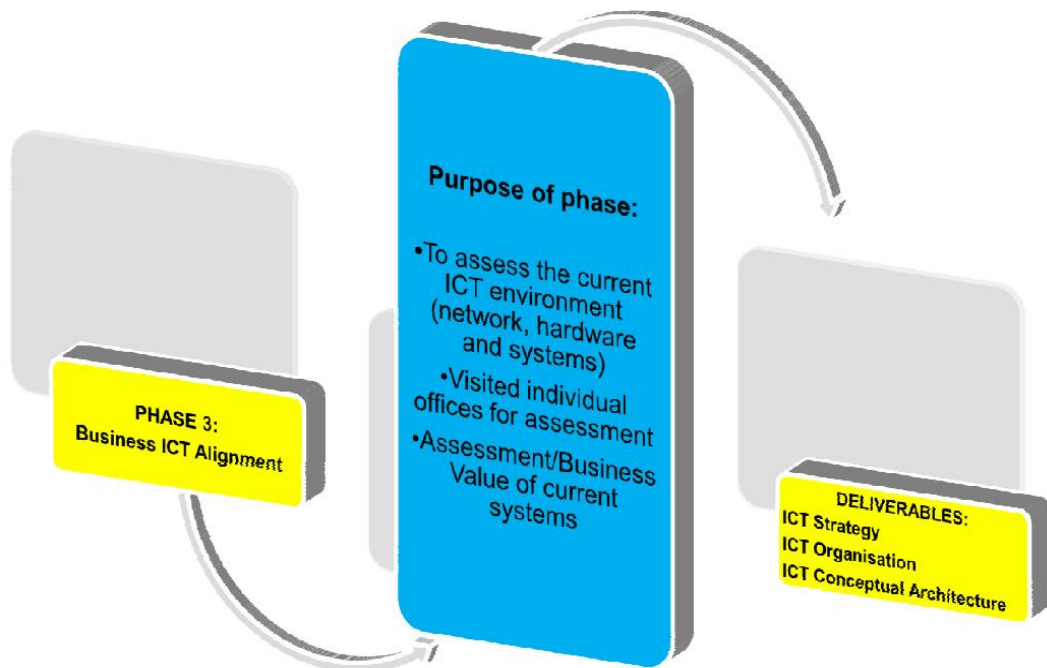
Strategic ICT Planning Framework: Business Strategy Articulation



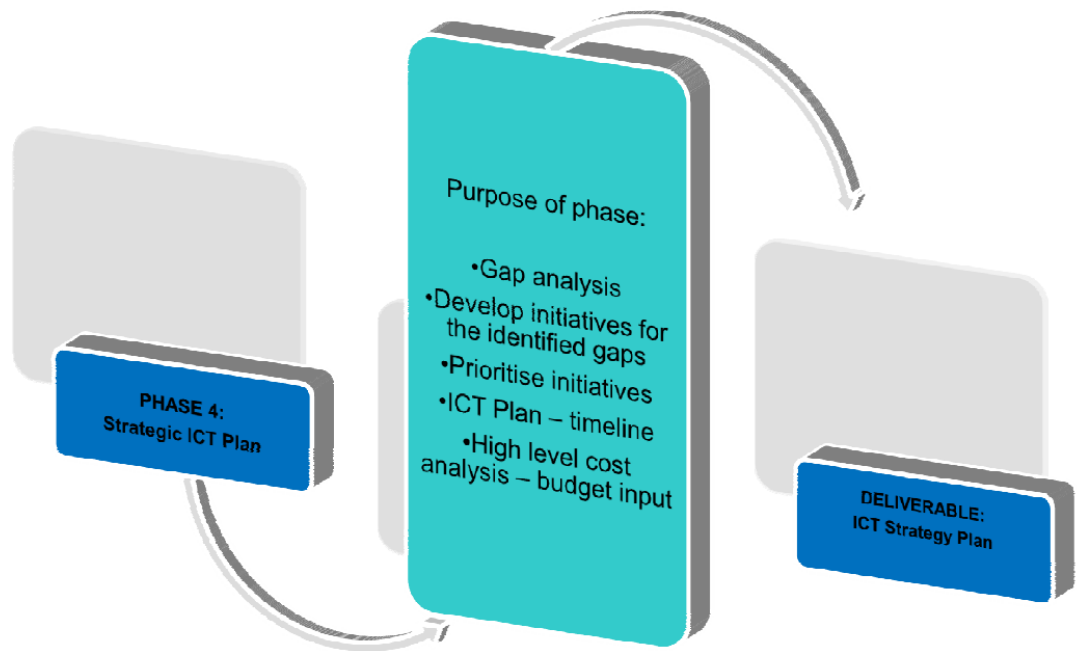
Strategic ICT Planning Framework: Current ICT Assessment



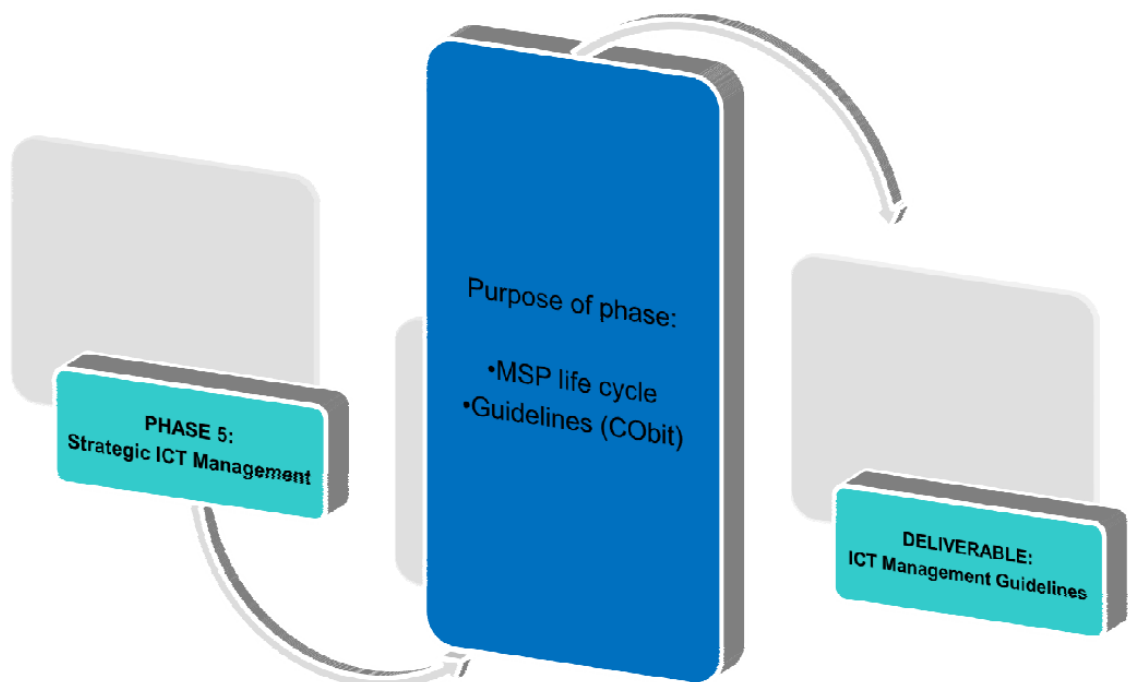
Strategic ICT Planning Framework: Business ICT Alignment



Strategic ICT Planning Framework: Strategic ICT Plan



Strategic ICT Planning Framework: Strategic ICT Management



3 ORGANISATIONAL STRUCTURE

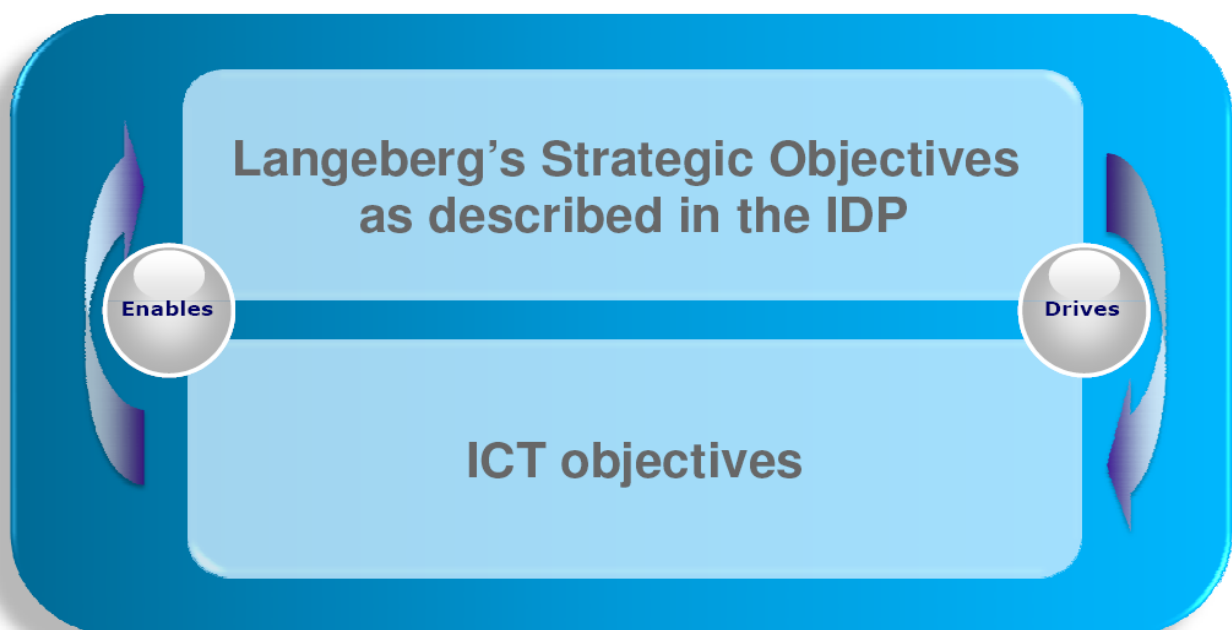


4 LINKING STRATEGIC DIRECTION

Legislative Mandate

- a) Constitution of the Republic of South Africa Act, 1996.
- b) Copyright Act, Act No. 98 of 1978
- c) Electronic Communications and Transactions Act, Act No. 25 of 2002
- d) Minimum Information Security Standards, as approved by Cabinet in 1996
- e) Municipal Finance Management Act, Act No. 56 of 2003
- f) Municipal Structures Act, Act No. 117 of 1998
- g) Municipal Systems Act, Act No. 32, of 2000
- h) National Archives and Record Service of South Africa Act, Act No. 43 of 1996
- i) National Archives Regulations and Guidance
- j) Promotion of Access to Information Act, Act No. 2 of 2000
- k) Protection of Personal Information Act, Act No. 4 of 2013
- l) The Cybercrimes Act 19 of 2020
- m) Regulation of Interception of Communications Act, Act No. 70 of 2002

Langeberg's Strategic Framework
objectives drives the ICT objectives



The ICT Strategic Objectives are encapsulated herein to respond to the Strategic Objectives as enshrined in the Municipality IDP document. In response to provide cost effective quality services to the Citizens, exercising good leadership, ensuring accountable governance, and maintaining sound

financial management. Our focus is building and maintaining our ICT infrastructure. The following ICT objectives have been formulated for Langeberg Municipality:

IDP Objective	ICT Objective	ICT Initiatives (2022 – 2027)
SO1: Ensure efficient administration for good governance	Improve and ensure a transformed ICT Governance within the Municipality.	Review all IT related policies and strategies. Installation of Standby Power Generators Develop and implement a Smart City Strategy
SO2: Provide infrastructure for sustainable and affordable basic services	Provide the necessary ICT infrastructure and network connectivity – “A Connected Langeberg”	Upgrade High-Site infrastructure. Upgrade ICT Core infrastructure (Servers, Storage, and Networks) A Connected Langeberg Voice Over Internet Protocol (VOIP) devices – telephone system Fibre to High Sites Rollout of Interbranch Fibre Connectivity Failover Internet Breakouts (per site) Public Wi-Fi (Strategic Municipal Sites) Two-Way Digital Radio Communication Network Two-Way Digital Radio Communication Network
SO3: Promote a safe and secure environment	Promote, uphold, and adhere to Cybersecurity and Business Continuity imperatives	Conduct Cybersecurity awareness. Ensure secure and up-to-date Cybersecurity controls on existing ICT infrastructure and systems. Conduct Cybersecurity assessments and remediation of findings thereof. Establish a Security Operations Center (insourced/outsourced). Develop an ICT Disaster Recovery Plan aligned to the Business Continuity Plan.
SO4: Promote and facilitate investment and local economic development	Facilitate ICT skills development and establish public-private partnerships.	Establish partnerships with ICT SETAs for skills development. Build public-private partnerships with other State-aligned institutions on ICT turnkey projects.
SO5: Provide sustainable financial	Ensure properly budgeted,	Conduct budget planning, project management, and SLA/contract management in-line with the relevant

management	affordable, and cost-effective ICT initiatives.	regulations.
------------	---	--------------

In response to business drivers, the following ICT Objectives have been formulated for Langeberg

ICT OBJECTIVE 01: IMPROVE AND ENSURE A TRANSFORMED ICT GOVERNANCE WITHIN THE MUNICIPALITY

- The ICT Governance structures, such as the Business Continuity Committee, Fraud and Risk Committee, and Audit and Performance Committee need to be continuously strengthened as both advisory and accounting bodies to the ICT unit.
- All ICT policies and strategies must be reviewed annually for approval by the Council to align with the ever-changing Municipality demands.
- To ensure continued ICT operations, all adequate and necessary supporting equipment must be sourced and well maintained.
- To align with the innovative and modern methodologies of basic service delivery, there is a need for ICT to be a strategic partner in sponsoring the technology and system concepts into the organizational Smart City Strategy.

ICT OBJECTIVE 02: PROVIDE THE NECESSARY ICT INFRASTRUCTURE AND NETWORK CONNECTIVITY – “A CONNECTED LANGEBERG”

- The internal and external network of the Langeberg ICT services should be kept relevant to modern standards and the quality of services remain optimum.
- The ICT infrastructure in place should cater for the ever-growing demands of the Municipality to ensure integrity, scalability, and responsiveness.
- The communications technologies in place should ensure the Municipality remains reachable and contactable at all times necessary.
- The ICT services should leverage the public-facing Municipality systems for adequate consumption and utilization.
- There should be adequate ICT-related tools in place to ensure that all Municipal personnel can respond to basic service delivery issues.

ICT OBJECTIVE 03: PROMOTE, UPHOLD, AND ADHERE TO CYBERSECURITY AND BUSINESS CONTINUITY IMPERATIVES

- The network of ICT services should always be kept up-to-date and secure to ensure maximum mitigation of potential cyber risks and threats.
- All Langeberg ICT system users should be made aware of the potential cyber risks and how to ensure housekeeping in anticipation of such for the protection and safety of the Municipal data and assets.

- The Langeberg ICT network should be continuously assessed in-line with regulated ICT security guidelines, benchmarks, and frameworks.
- All ICT Practitioners and service providers should be kept competent and alive to cybersecurity initiatives to allow for efficient responses and handling of related matters.
- To ensure that the Municipality continues to offer its primary mandate, basic service delivery, there must always be plans in place on how to recover from potential disasters within the adequate period with the integrity of systems kept intact.

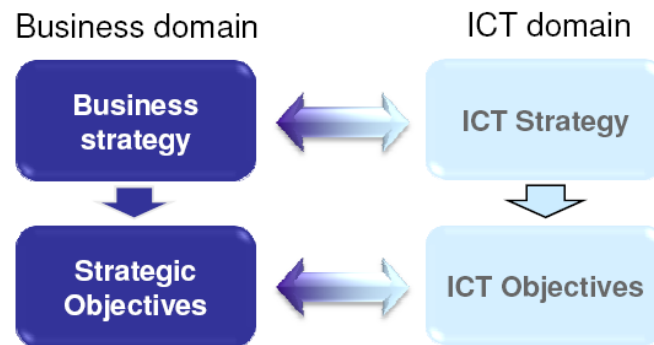
ICT OBJECTIVE 04: FACILITATE ICT SKILLS DEVELOPMENT AND ESTABLISH PUBLIC-PRIVATE PARTNERSHIPS

- The ICT unit should play a pivotal role in ensuring that the ICT skills requirements are well maintained and optimized where necessary.
- The skills development initiatives should be achieved in-line with the Workplace Skills Plan and the engagement of ICT SETAs for the provisioning of ICT training.
- Establish public-private partnerships for macro-scale turnkey projects and other strategic ICT initiatives to ease pressure on Municipal fiscus and share operational responsibility for the benefit of the public.

ICT OBJECTIVE 05: ENSURE PROPERLY BUDGETED, AFFORDABLE, AND COST-EFFECTIVE ICT INITIATIVES

- Develop business plans in-line with the IDP strategic objectives.
- Ensure structured, productive, and cost-effective project management.
- Ensure service level agreements and contract assessment with existing ICT service providers with strict adherence to the relevant legislations and regulations.

Strategic alignment model used to align the ICT Strategy



- The primary objective of this approach is to align the future ICT environment on a strategic level
- The above interaction between business and ICT sets out to answer the following key questions;
 - What should ICT do to enable business to execute its strategy?
 - What should ICT do to enable business to accomplish its Strategic objectives?
 - What can ICT do to enhance service delivery?
 - How should ICT be governed to ensure continued alignment?

Strategy Alignment Framework – Ventrakaman [1993]

Langeberg Vision and Mission

Vision

To create a safe and healthy environment for delivering sustainable quality services



Mission

An efficient and cost-effective municipality for good governance, sustainable services, safe and secure environment, sound financial management and a conducive environment for local economic development.

Langeberg ICT Vision and ICT Mission

Vision

To be the innovative resource that continuously enhances service delivery through the application of innovative information and technology.



Mission

To provide an effective and efficient support service to the municipal directorates so that the organisational objectives can be achieved through the provision of ICT and sound International and Intergovernmental relations.

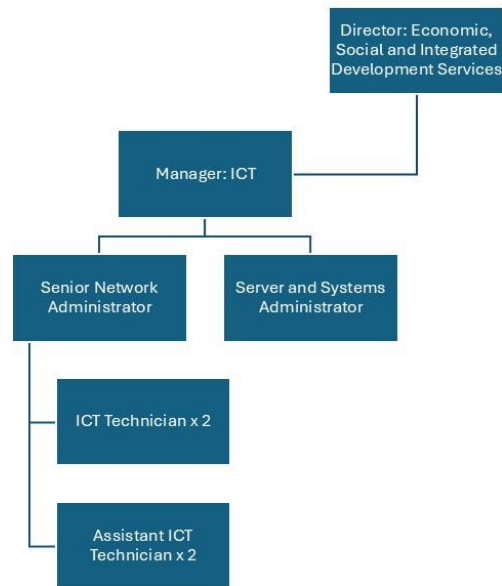
To provide a high-quality network that supports the current and future essential network and applications of the municipality, as well as telecommunication services in voice, video, and data.

We are dedicated to ensuring the integrity of data, improving services delivery, and fostering a bright technological future for Langeberg Municipality.

To improve and enhance the IT platform in alignment with the need for business to improve productivity.

To ensure that the business objectives of delivering services to the community are met by the Langeberg Municipality.

Current Langeberg Municipality ICT Organization

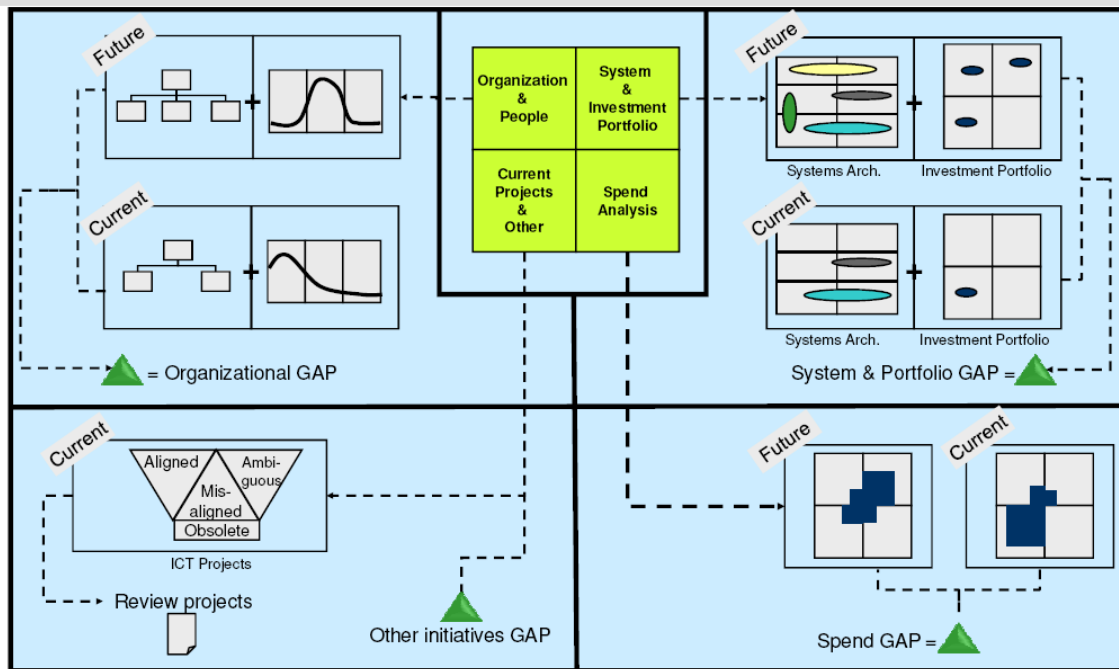


Langeberg Municipality uses the following business systems

BUSINESS UNIT SYSTEMS	FINANCE SERVICES	ECONOMIC, SOCIAL AND INTEGRATED DEVELOPMENT SERVICES	CORPORATE SERVICES	ENGINEERING SERVICES	COMMUNITY SERVICES	OFFICE OF THE MUNICIPAL MANAGER
PROMUN	√			√		
SAGE ERP	√	√	√	√	√	√
COLLABORATOR	√	√	√	√	√	√
S3	√	√	√	√		
IGNITE	√	√	√	√	√	√
WINDEED	√		√	√	√	
CAD				√		
TCS			√			
MS TEAMS	√	√	√	√	√	√
MS OFFICE	√	√	√	√	√	√
E-MAIL	√	√	√	√	√	√

Note: The PROMUN system was replaced by the Sage ERP system as a Financial System of the Langeberg Municipality. The Municipality keeps the PROMUN data for archive and reference purposes.

The gap analysis is performed on the following four areas to determine a collective list of ICT and related initiatives



Risk Management

The management of risks is a cornerstone of ICT Governance, ensuring that the strategic objectives of the business are not jeopardised by ICT failures. ICT related risks are increasingly a, Business Continuity Committee\SMT level issue as the impact on the organisation of an ICT failure, be it an operational crash, security breach or a failed project, can have devastating consequences. However, managing ICT risks and exercising proper governance is a challenging experience for business managers faced with technical complexity, a dependence on an increasing number of service providers, and limited reliable risk monitoring information. As a consequence, management is often concerned whether risks are being cost effectively addressed, and they need assurance that risks are under control.

Therefore, the steering committee should manage enterprise risk by:

- a) Ascertaining that there is transparency about the significant risks to the enterprise and clarifying the risk-taking or risk-avoidance policies of the enterprise.
- b) Being aware that the final responsibility for risk management rests with the steering committee so, when delegating to executive management, making sure the constraints of that delegation are communicated and clearly understood.
- c) Being conscious that the system of internal control put in place to manage risks often has the capacity to generate cost-efficiency.
- d) Considering that a transparent and proactive risk management approach can create competitive advantage that can be exploited.
- e) Insisting that risk management is embedded in the operation of the enterprise, responds quickly to changing risks and reports immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).

We must be conscious though that risk taking is an essential element of business today. Success will come to those organisations that identify and manage risks most effectively. Risk is as much about failing to grasp an opportunity as it is about doing something badly or incorrectly.

5 ICT STRUCTURE

The growing interest in ICT Governance and increasing pressure to deal with regulatory compliance and a continuing focus on security has made ICT management much more involved in risk management and control activities. There is therefore a need for ICT management to work more closely with the auditors.

6 LIST OF CURRENT APPLICATIONS / SYSTEMS IN USE

Executive management has a responsibility to ensure that the organisation provides all users with a secure information systems environment. Sound security is fundamental to achieving this assurance. Information systems can generate many direct and indirect benefits, and as many direct and indirect risks. These risks have led to a gap between the need to protect systems and the degree of protection applied. Proper governance of security, like any other aspect of ICT, requires top management to be more involved in setting direction and overseeing the management of risk.

7 GAP ANALYSIS

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 the 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 not be edited. The municipality uses security applications, Firewalls, to detect and prevent electronic viruses.

The Municipality must have a patch management framework in place. This would reduce and mitigate the vulnerability and compromise of Municipality systems.. If the municipality allows wireless access, it must be appropriately controlled and/or 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:

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

8 ICT LIFECYCLE

The Municipality must have internal controls over the management of information assets which appear satisfactory. The Municipality must keep an asset register, which requires to be updated regularly 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 unauthorized changes by limiting access rights.

The server room must be equipped with at least an air conditioner, UPS and smoke detectors to protect it from environmental hazards such as flooding, fire, and power outages. The Municipality should continue enforcing good practices with regards to physical security and environment controls.

9 Business Continuity Management

The security management of the Municipality should ensure that the information risk assessment is conducted to inform the municipality Business Continuity Plan and ICT Disaster Recovery Plan:

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

10 ICT Governance Framework Decision Making Process

The following structures and related roles and responsibilities are institutionalised in the municipality:

Structure	Role	Responsibility
Municipal Council	Executive Leadership	1. Determine the Municipal Governance of ICT Policy. This includes formulating the strategic intent of digital evolution and oversight for value creation and risk management. 2. Monitor: a. The effectiveness of the governance system, b. That IDP includes business enablement, and that value is realised, c. That municipality can recover from disruptive incidents (including cyber), d. That sufficient technology skills are provided, e. The sufficiency of information systems architecture. 3. Ensure confidence that a fit-for-purpose, business-enabling ICT functional structure is established. 4. Providing strategic oversight that municipal data is ethically managed, legally compliant, aligned with service delivery goals, and supports evidence-based decision-making. 5. Allocate and approve budget.
Municipal Manager	Accounting Officer	1. Provide strategic guidance and oversight of digital evolution. 2. Inform and approve the Business Enabling ICT Plan, business cases, and the related Municipal ICT Management Framework. 3. Coordinate responsibilities of the Business Continuity Committee. 4. Ensure business enabling risk management and independent assurance. 5. Establish the ICT function and its related organisational structure. 6. Coordinate institutionalisation and maintenance of compliant, secure, and effective data management practices. 7. Propose business enabling budget to Council. 8. Coordinate reporting for Council oversight.
Business Continuity Committee	Coordinating and Oversight Forum	1. Oversee and inform the development of the prioritised business enabling Business Enabling ICT Plan and related business cases. 2. Advise strategic leadership and the municipal manager on the adoption of the Business Enabling ICT Plan and business cases. 3. Coordinate the implementation of the Business Enabling ICT Plan. 4. Coordinate, oversee, and inform the development of an enabling budget, taking into consideration life-cycle management. 5. Coordinate the implementation of the Business Enabling ICT Plan 6. Coordinate digital ecosystem risk management and maintain risk register.

Structure	Role	Responsibility
		7. Consider and decide on digital operational matters. 8. Ensure business, application system, and technology architectural fit of current digital ecosystem and future business solutions. 9. Coordinate the resolution of related audit findings. 10. Oversee related service provider performance management. 11. Coordinate information system and technology change management. 12. Report on Council oversight monitoring mechanisms (see 8 above).
Municipal Risk Committee (Fraud and Risk Management Committee)	Oversight of business-related ICT strategic, management, and operational risk.	1. Oversee that digital ecosystem is appropriately managed. 2. Oversee management of cybersecurity risk. 3. Advise all related structures on risk, emerging risk, and risk management. 4. Assist the business and ICT function to clearly define risks and allocate risk owners.
Municipal Audit and Performance Committee (Audit and Performance Committee)	Oversight of establishment of risk appropriate controls	1. Oversee and advise on prescriptive compliance. 2. Advise on the effectiveness of risk appropriate controls and its shortcomings. 3. Evaluate effectiveness of municipal resilience, continuity, and cyber security measures and provide related advice.
Business Management	Information Management System Owner	1. Perform information system ownership responsibilities, which include: a) the solutions addressing business needs, b) that solutions are business functional, c) user access and use rights allocation, and d) that the aspects of the ICT operational frameworks/policies that apply are adhered to e) manage service provider performance. 2. Inform business enabling information system continuity requirements and related ICT continuity testing. 3. As part of the Business Continuity Committee, collaborate with the ICT Manager to develop the business enabling ICT initiatives, formulate business cases, and plan the implementation of the digital ecosystem with related budget, taking into consideration a) functional requirements and technological capabilities, and b) business and ICT skills development. 4. Coordinate information system change management. 5. Determine and manage business and ICT service level agreements. 6. Performance manage related service providers.
ICT Manager	Leadership of the ICT Function and business and ICT relationships	1. With the business, align the use of technology, skills, and effort with business enabling requirements. 2. Manage ICT function in the municipality. 3. Monitor and evaluate ICT function effectiveness and compliance. 4. Inform information system and determine technology life cycle management. 5. Lead technological ICT continuity management.

10.1 Decision Rights

Critical components of an ICT governance framework are the clear definition of decision rights and a process by which decisions are made. A framework outlines the roles and relationships amongst these groups.

Langeberg Municipality's ICT Governance Framework utilizes the Responsibility Assignment Matrix to define decision rights. Roles in this decision-making framework, commonly referred to as RACI Matrix, fall into one of four distinct categories: Responsible (R), Accountable (A), Consulted (C), or Informed (I).

The following applies:

Role-Player	Municipal Council	Municipal Manager	Other Executive Directors	Director: Economic, Social and Integrated Development Services	Chief Financial Officer	Subject Matter Expert	Business Solution Owner	ICT Manager	Chairperson of the Business Continuity Committee	Manager: IDP, Performance and	Chief Audit Executive	Audit and Performance Committee	Risk Champions	Fraud and Risk Management Committee
Tasks														
Municipal Governance of ICT Policy	A	R	C	C	I	I	I	C	I	I	I	I	C	I
Municipal Governance of ICT Charter	A	R	C	C	I	I	I	C	I	I	I	I	C	I
Municipal ICT Management Framework	N/A	A	I	I	I	I	C	R	C	N/A	I	I	I	I
Municipal ICT Management Pillars	N/A	A	I	I	C	I	C	R	I	N/A	I	I	I	I
Individual Business Cases	N/A	A	C	C	C	I	C	C	R	N/A	I	I	I	I
Funded business cases reflected in the IDP	I	A	R	C	C	C	C	C	I	I	I	I	C	I
Business Enabling ICT Plan (Derived from approved business cases in the IDP)	I	I	A	C	I	I	I	C	C	R	I	I	I	I
Project Plan (Per Project)	I	A	R	R	R	C	C		I	C	I	I	C	I
Architecture Management (Application Portfolio, Back Office, Network)	N/A	I	A	C	C	R	R	C	I	N/A	I	I	C	I
Strategic Risk Register	N/A	I	R	A	R	R	R	R	I	N/A	I	N/A	I	N/A
Operational Risk Register	I	A	R	R	R	C	N/A	C	C	I	I	I	I	I
Business functional fit of application systems (Per application)	N/A	N/A	I	A	C	C	C	C	C	N/A	I	I	C	I

Role-Player	Fraud and Risk Management Committee	Risk Champions	Audit and Performance Committee	Chief Audit Executive	Manager: IDP, Performance and	Chairperson of the Business Continuity Committee	ICT Manager	Business Solution Owner	Subject Matter Expert	Chief Financial Officer	Director: Economic, Social and Integrated Development Services	Other Executive Directors	Municipal Manager	Municipal Council
system)														
Supplier performance management (Per application system)	I	I	I	I	N/A	I	C	C	R	A	A	A	I	I
Master and Service Level Agreements (Per solution/application system)	C	C	C	C	N/A	C	R	R	C	A	A	A	I	N/A
Functional fit of the ICT business unit	I	I	I	I	N/A	I	R	R	C	R	R	R	A	I
Digital skills development (both in the business and ICT)	I	I	I	I	N/A	I	C	R	C	R	R	R	R	A
Business Continuity to Inform ICT Continuity	I	I	I	I	N/A	I	C	C	C	R	R	R	A	I
ICT Disaster Recovery Plan	C	I	C	I	N/A	C	C	C	C	R	R	R	A	I
Data Governance (Confidentiality, Integrity, Availability)	C	I	C	I	N/A	C	R	C	C	R	A	R	C	I
Information System Architecture Capacity Management	C	I	C	I	N/A	I	C	C	C	R	R	R	A	I
Information System Architecture Capacity Management	I	I	I	I	N/A	I	R	R	R	C	A	C	I	I

10.2 Resource requirements and services

Imperative	Business requirements
Affordability	Public sector entities require IT costs to be low and are focused on value for money. The benefits received from the IT environment should outweigh the cost. Costs of ownership and operating costs should be low in order to utilise taxpayers' money efficiently in transforming it into tangible outcomes for society.
Agility	The IT systems should be able (flexible) to adapt to changes in political power, restructuring possibilities and changes in the economy. The IT systems should also be able to adapt to provide easier methods of interaction with the citizens.
Ease of use	The IT technology should be easy to use for all users. It should not be too complex, which could lead to idle time, mistakes and the requirement for highly skilled staff. Since decisions are made based on information captured it is important to limit mistakes. The entities also want to limit unnecessary expenditure on IT training caused by complex systems.
Reliability	Systems need to function as intended at all times to be available, effective and efficient.
Security	Access to the personal data of citizens should be safeguarded to prevent unauthorised access to such information. Unauthorised transactions should also be prevented.
Self service	Entities want citizens to be able to perform certain tasks (such as register for tax purposes) directly and quickly themselves.

10.3 Roles and Responsibility Categories

Functional Level	Designation
Strategic	Municipal Manager, Director: ESIDS, and Manager: ICT
Tactical	Director: ESIDS
	Internal Audit
Operational	Business Process Owner

10.4 Vision, Planning and Operations Governance

According to Chapter 5 of the King III code of good governance, focusing specifically on ICT, the table below recommends best practices for each category.

Principles	Recommended Practice
The Business Continuity Committee should be responsible for ICT (ICT) governance.	The Business Continuity Committee should assume the responsibility for the governance of ICT and place it on the Business Continuity Committee agenda. The Business Continuity Committee should ensure that an ICT Charter and Policies are established and implemented. The Business Continuity Committee should ensure promotion of an ethical governance culture and awareness and of a common ICT Language. The Business Continuity Committee should ensure that an ICT internal control framework is adopted and implemented. The Business Continuity Committee should receive independent assurance of the effectiveness of the ICT internal controls.
ICT should be aligned with the performance and sustainability objectives of the Municipality	The Business Continuity Committee should ensure that the ICT Strategy is integrated with the company's strategic and business processes. The Business Continuity Committee should ensure that there is a process in place to identify and exploit opportunities to improve the performance and sustainability of the Municipality through the use of ICT.
The Accounting Officer should delegate to management the responsibility for the implementation of an ICT Governance Framework	Management should be responsible for the implementation of the structures, processes and mechanisms for the ICT Governance Framework. The Accounting Officer may appoint an Business Continuity Committee\SMT of similar function to assist with its governance of ICT. The Accounting Officer should appoint Director: ESIDS/Manager: ICT responsible for the management of ICT. The Director: ESIDS/Manager: ICT should be a suitably qualified and experienced person who should have access and interact regularly on strategic ICT matters.
The Business Continuity Committee should monitor and evaluate significant investments and expenditure	The Business Continuity Committee should oversee the value delivery of ICT and monitor the return on investment from significant ICT projects. The Business Continuity Committee should ensure that intellectual property contained in information systems is protected. The Business Continuity Committee should obtain independent assurance on the ICT governance and controls supporting outsourced ICT services.
ICT Should form an integral part of the Municipality risk management	Management should regularly demonstrate to the Business Continuity Committee that the company has adequate business resilience arrangements in place for disaster recovery. The Business Continuity Committee should ensure that the Municipality complies with ICT laws and that ICT related rules, codes and standards are considered.

10.5 Defined Processes

The Business Continuity Committee should ensure that information assets are managed effectively	The Business Continuity Committee should ensure that there are systems in place for the management of information which should include information security, information management and information privacy. The Business Continuity Committee should ensure that all personal information is treated by the company as an important business asset and is identified.
A Fraud and Risk Management Committee (FARMCO) and Audit and Performance Committee (APC) should assist the Business Continuity Committee in carrying out its ICT responsibilities	The FARMCO should ensure that ICT Risks are adequately addressed. The FARMCO should obtain appropriate assurance that controls are in place and effective in addressing ICT risks. The APC should consider ICT as it relates to financial reporting and the going concern of the Municipality. The APC should consider the use of technology to improve audit coverage and efficiency.

The Business Continuity Committee\SMT was established to provide advice to the MM/Director: ESIDS/Manager: ICT. The Business Continuity Committee\SMT serves the MM/Director: ESIDS/Manager: ICT in a consultative capacity. The committee is required to advise the MM/Director: ESIDS/Manager: ICT on a broad array of topics including, but not limited to:

- a) Development and implementation of the Municipal ICT strategic plan
- b) Critical ICT initiatives for the Municipality
- c) Standards for Municipal Information Architecture
- d) Identification of business and technical needs of Municipal departments
- e) Strategic ICT portfolio management, project prioritization and investment decisions
- f) Municipal ICT performance measures and fees for service agreements
- g) Management of the Municipal ICT budget
- h) The efficient and effective operation of the office

The Business Continuity Committee meetings and agenda are managed by the office of the MM/Director: ESIDS/Manager: ICT. To fulfill its diverse statutory responsibilities, the Business Continuity Committee\SMT will conduct ongoing meetings to gain an understanding of and provide insight into key technology decisions. Agendas for Business Continuity Committee meetings will include regular reports on governing activity and decision points as well as significant management decisions that do not flow through governance, such as budgeting and rate setting of ICT Services.

10.6 The Business Continuity Committee

The purpose of the ICT Steering Committee is, as a group responsible for providing executive leadership in the development of standards, policies, and the prioritization of various initiatives. The Executive Business Continuity Committee will provide a stabilizing influence so that organizational concepts and directions are established and maintained with a visionary view. The Business Continuity Committee provides direction on long-term strategies in support of the Municipality's mandates and business vision. Members of the Business Continuity Committee ensure that the Municipality's Information and Communication Technology needs and objectives are being adequately addressed.

10.7 Business Continuity Committee Responsibilities

The Business Continuity Committee is responsible for:



- a) Ensuring clear scope and Terms of Reference;
- b) Providing necessary resources to achieve desired outcomes;
- c) Conflict resolution;
- d) Risk Management;
- e) Ensuring the committee achieves pre-defined objectives/targets

10.8 Business Continuity Committee Membership

It is critically important to have key stakeholders involved in the Business Continuity Committee. These stakeholders are representatives from both business as well as ICT. It is recommended that the Business Continuity Committee comprises of the following persons or representatives thereof:

- a) Municipal Manager – Business Continuity Committee Chairperson
- b) Director: Financial Services (CFO)
- c) Director: Economic, Social and Integrated Development Services
- d) Director: Community Services
- e) Director: Corporate Services
- f) Director: Engineering Services
- g) Chief Audit Executive – Business Continuity Committee Administrator
- h) Chief Fire Officer – Business Continuity Committee Operational Command Coordinator
- i) Manager: ICT
- j) Risk Champions – Manager: Expenditure, Manager: IDP, Performance Management, and communications, Manager: Electrical Services, Manager: Community Facilities, and Manager: Law Enforcement.

The SLA assessment function of the BCC is managed through a Special Business Continuity Committee meeting to formulate a report. The Special BCC is recommended to comprise of the following persons or representatives:

- a) Director: Economic, Social and Integrated Development Services – Chairperson
- b) Director: Financial Services (CFO)
- c) Chief Audit Executive
- d) Manager: ICT
- e) ICT-related Service Providers

10.9 Frequency and Scheduling of Meetings

Quarterly.

11 Reference List

- a) Boshoff, W. 2010. IT Governance and IT Assurance. Masters in Commerce (Computer Auditing) lecture slides, Langeberg University, Langeberg.
- b) DPSA (Department for Public Service and Administration). 1997. Batho Pele – Together beating the drum for service delivery [Online]. Available: <http://www.dpsa.gov.za/batho-pele/Principles.asp> [2011. July 21].
- c) IODSA (Institute of Directors Southern Africa). 2009. King Report on corporate governance for South Africa (King III) [Online]. Available: <http://www.iodsa.co.za> [2011, May 24].
- d) ISACA (Information Systems Audit and Control Association). 2008. Top business/technology issues - Survey results [Online]. Available: <http://www.isaca.org/Knowledge-Center/Research/Documents/Top-Business-Technology-Survey-Results.pdf> [2011, July 20].
- e) ITGI (IT Governance Institute). 2003. Board briefing on IT governance [Online]. Available: <http://www.itgi.org> [2011, May 24].
- f) ITGI (IT Governance Institute). 2005. IT alignment: Who is in charge? [Online]. Available: <http://www.isaca.org/Knowledge-Center/Research/Documents/ITAlignment-Who-Is-in-Charge.pdf> [2011, June 8].
- g) ITGI (IT Governance Institute). 2008a. Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit
- h) – A management briefing from ITGI and OGC [Online]. Available : http://www.itgi.org/template_ITGI275e.html?Section=Recent_Publications&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=43&ContentID=14046 [2011, May 25].
- i) ITGI (IT Governance Institute). 2008b. IT governance global status report – 2008 [Online]. Available: <http://www.isaca.org/Knowledge-Center/Research/Documents/ITGI-Global-Status-Report-2008.pdf> [2011, June 8]. Langeberg University <http://scholar.sun.ac.za>
- k) ITGI (IT Governance Institute). 2008c. Understanding how business goals drive IT goals [Online]. Available: <http://www.isaca.org/Knowledge-Center/Research/Documents/Understand-Bus-Drive-IT-Goals-15Oct08-Research.pdf> [2011, June 8].
- l) IT governance Institute (ITGI). 2011. Global status report on the governance of IT (CGEIT) – 2011 [Online]. Available: <http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf> [2011, July 23].
- m) ITGI & OGC (IT Governance Institute & Office of Government Commerce). 2005. Aligning Cobit, ITIL and ISO 17799 for business benefit: Management summary [Online]. Available: <http://www.itgovernance.co.uk/files/ITIL-COBiTISO17799JointFramework.pdf> [2011, May 25]. PWC (PricewaterhouseCoopers). 2009. King's Counsel. King III: A municipal perspective – at a glance [Online]. Available: <http://www.pwc.com/za/en/publications/steering-point.jhtml#SteeringPoint> [2011, May 26].
- n) Le Roux, F. 2010. The applicability of the Third King Report on Corporate Governance to small and medium enterprises [Online]. Available: <http://www.scholar.sun.ac.za/handle/10019.1/1017> [2011, May 25].
- o) PWC (PricewaterhouseCoopers). 2010a. IT governance [Online]. Available:

- p) PWC (PricewaterhouseCoopers). 2010b. King's Counsel. Understanding and unlocking the benefits of sound corporate governance in government and the public sector [Online]. Available: <http://www.pwc.com/za/en/publications/steeringpoint.jhtml#SteeringPoint> [2011, May 26].
- q) PWC (PricewaterhouseCoopers). 2010c. King III and related legislative requirements [Online]. Available: <http://www.pwc.com/za/en/publications/steeringpoint> [2011, May 26].
- r) Woods, S. 2010. Governing IT in the public sector [Online]. Available: <http://www.itnewsafrika.com/2010/08/governing-it-in-the-public-sector/> [2011, May 26].
- s) KPMG – KING IV <https://home.kpmg/za/en/home/insights/2016/10/king-iv-report-on-corporate-governance-for-south-africa-2016.html>
- t) Protection of Personal Information Act 4 of 2013
<https://www.gov.za/documents/protection-personal-information-act>
- u) The Cybercrimes Act 19 of 2020
<https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000>

12 Endorsement

The Municipal Manager / Accounting Officer by virtue of his/her signature hereby ENDORSES this policy.

The Mayor / Speaker by virtue of his signature, on behalf of the Council of Langeberg Municipality and after presentation of this policy before Council hereby APPROVE this policy.

Reviewed by:

March 2026

MR B BAKACO

DATE

Manager: ICT

13 Document History

Effective Date: _____

Revision History			
Revision	Date	Description of changes	Requested By
Council	March 2020	Resource requirements and the services	Zaine Prins As per Action Plan of 2018/2019 External Audit Findings
Council	March 2022	ICT Strategic Objectives	Zaine Prins
Council	March 2023	Compliance to POPI Act , Cybercrime Act and Personal Devices (BYOD)	Zaine Prins As per Audit Action Plan in Internal Audit Findings: Economic, Social and Integrated Development Services Internal Audit Findings on 2021/22 Audit on Cybercrime (Report reference: 6441)
Council	March 2024	Alignment of ICT Strategic Objectives to IDP Strategic Objectives	Manager: ICT
Council	March 2026	Update of the Organisational Structure due to the name change of the SSD Directorate to ESIDS. Alignment of Strategy Plan to Municipal Governance of ICT Framework Updating of the revised ICT organisational structure	Manager: ICT