Western Cape Government

CAPE AGULHAS MUNICIPALITY

ICT STRATEGY & IMPLEMENTATION PLAN 2017 - 2022

Kaap Agulhas Munisipaliteit
Cape Agulhas Municipality
U Masipala Wasecape Agulhas

Municipality & Office Details

Cape Agulhas Municipality
Dirkie Uysstreet 1
Bredasdorp
7280
028 425 5500
Herein after known and identified as 'the municipality'.

Document Authorization

The parties hereto as below duly authorize upon their signature the acceptance of all items contained herein and annexed hereto.

DGI O'NEILL		14/02/2018
Chairperson: Municipal ICT Steering Committee	Signature	Date
DGI O'NEILL		14/02/2018
Municipal Manager	Signature	Date
G.S. BURGER.		14/02/2018
Council Portfolio Chair	Signature	Date
D.J. Swart		14/02/2018
Mayor	Signature	Date

Approved by:	Council	**Resolution number:**	250/2017
Approval date:	07/12/2017	**Review date:**	DD / MM / YYYY

Copyright

Version Management

Document Control			
Document Date:	23 November 2017	**Lifecycle:**	Strategy & Implementation Plan (5 Years)
Version Contributor:	DLG & Municipalities	**Capacity:**	Project Directors & Workshop Stakeholders.
Change Control:	Working document 1 – Municipal ICT inputs.		

Glossary

AG	Auditor-General of South Africa
ADM	Architecture Development Method
BROADBAND	High Speed Internet Access
BRM	Benefits Realization Management
CMMI	Capability Maturity Model Integration
BSC	Balanced Score Card
CGICTPF	Corporate Governance of ICT Policy Framework
CGICT	Corporate Governance of ICT
COBIT®	Control Objectives for Information Technology
EA	Enterprise Architecture
ERP	Enterprise Resource Planning
FMS	Financial Management System
GICT	Governance of ICT
ICT	Information and Communications Technology
IDP	Integrated Development Plan
ISACA®	Information Systems Audit and Control Association
ISO 38500	International Organisation for Standardization (38500)
ISCGICT	International Standard on Corporate Governance of ICT
ITGI™	IT Governance Institute
ITIL	The Information Technology Infrastructure Library
King III	The King III Report and Code on Governance for South Africa
MCA	Municipal Charter of Accounts
MICTGPF	Municipal ICT Governance Policy Framework
MCGICTP	Municipal Corporate Governance of Information and Communication Technology Policy
MICTSIP	Municipal ICT Strategy and Implementation Plan
MIS	Management Information System
mSCOA	Municipal Standard Charter of Accounts
M&E	Monitoring and Evaluation
NDP	National Development Plan
OS	Operating System(s)
PFD	Process Flow Diagram
PSCGICTPF	Public Service Corporate ICT Governance Policy Framework
SALGA	South African Local Government Association

SDBIP	Service Delivery and Budget Implementation Plan
SOP	Standard Operating Procedure
SOW	Scope of Work
TOGAF®	The Open Group Architecture Framework
ZACHMAN	The Zachman Framework

TABLE OF CONTENTS

VIA ADDENDUM

1 Consideration

This ICT strategy has been developed and delivers on Phase One (1) and Phase Two (2) of the Municipal Corporate Governance of Information and Communication Technology Policy (MCGICTP) that has been circulated by COGTA and subsequently approved by the municipality.

There are numerous components that make up and contribute towards this document which may be noted as single framework as established below.

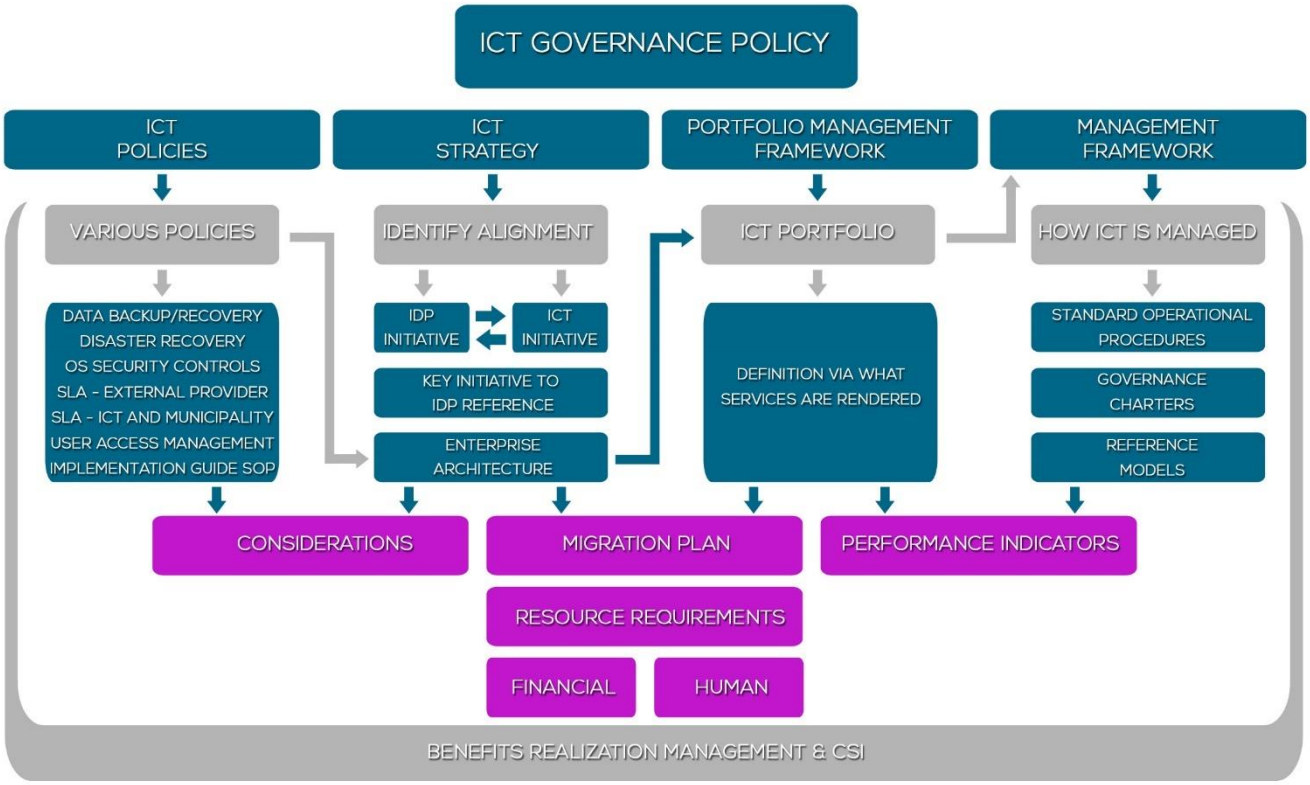

Figure 1: Holistic ICT Governance Framework.

The legend below will provide context around how the above framework may be understood:

Primary Drivers

Linkages

Intentions or Outcomes

The Holistic ICT Governance Framework above provides an overview from a top-down format on the flow of all components embodied within the framework. The framework provides a linear view on the approach towards moving forward aggressively through context of *Primary Drivers, Linkages* with *Intentions or Outcomes* and how their interrelations are viewed or reviewed. This will assist the municipality with an easily understandable model as to how and where items are situated or positioned.

2 Preface

This document shall officiate all aspects around the Municipal Information and Communications Technology Strategy & Implementation Plan (MICTSIP). It will be used as a standard for ensuring alignment of the municipal IDP with the objectives of Information and Communications Technology (ICT) through a governed and unified standard. This strategy document therefore exists parallel to the IDP, and should be reviewed in alignment with the IDP review processes. The framework within the context of which this document conforms to is as noted below.

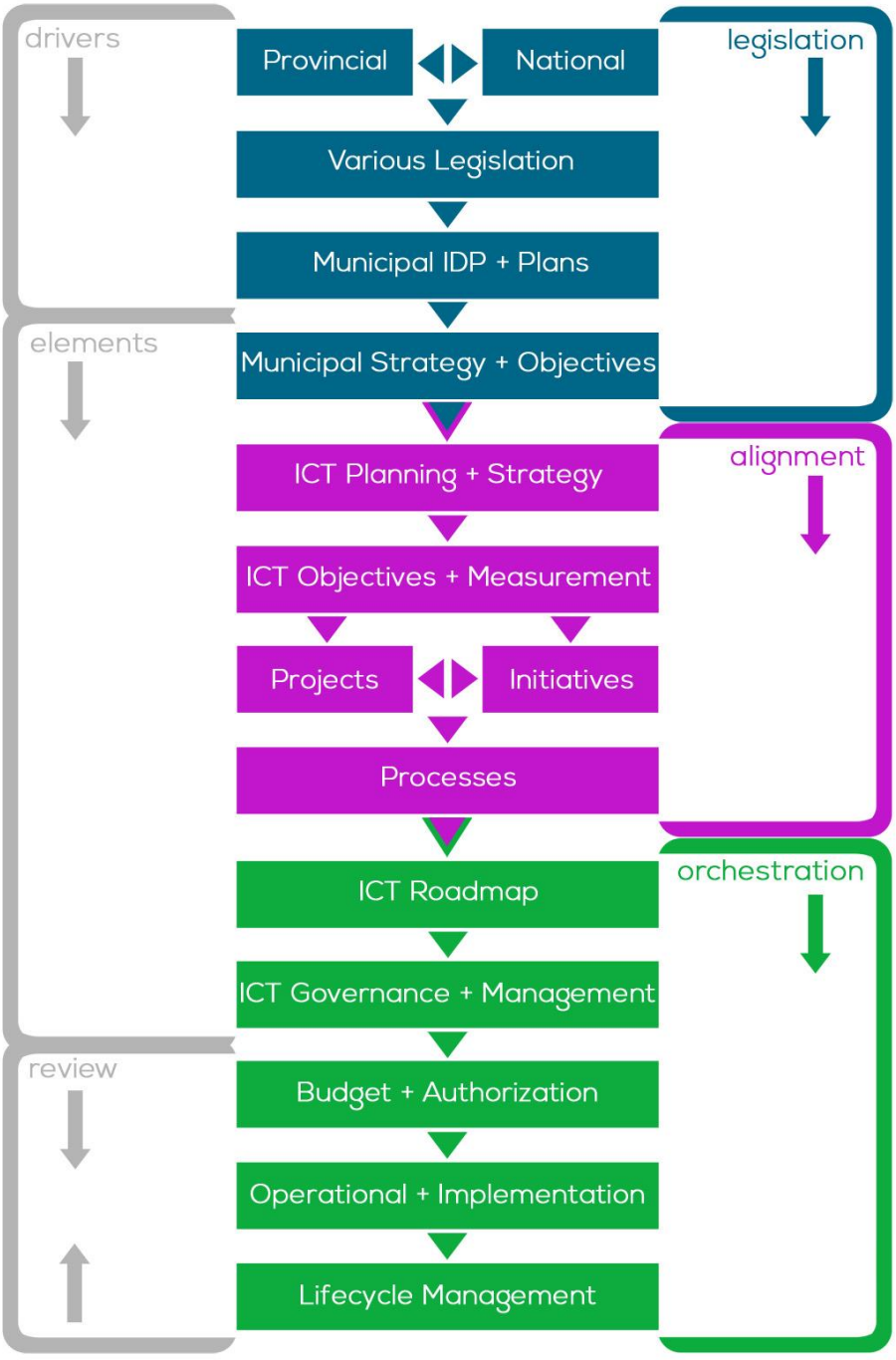

Figure 2: Structure - MICTSIP Framework, Process Flow Diagram (PFD).

The PFD above shall guide the narrative towards the structure and context of this document, whereas the lifecycle below will dictate the overarching process as a continual and ongoing asset to the MICTSIP framework.

Figure 3: Structure - MICTSIP Lifecycle.

The preceding items within this document will speak specifically to the municipality; whereby upon its completion through finalizing of all required content, it will identify the unique requirements and set forth all required procedures for actualization of meeting the ICT objectives of the municipality and its stakeholders.

This document will be noted formally and officially as a strategy, which will be set in place for a period of five (5) years. May it be noted that the implementation plans contained within this document will yield a turnaround of a five (5) year period for holistic conclusion; however, any additional ICT undertakings during the five (5) year lifecycle of this strategy shall specifically comply to all governance as set out within this document.

Any reform related to legislation, will however be considered if it has direct impact on the governance, framework, process flow or lifecycle contained within this document.

3 Executive Summary

The Municipality has during its IDP development processes for the period of 2017 - 2022, committed to enhancing service delivery and engagement around citizenry. During the IDP planning processes it identified a key to its delivery is commitment to the Batho Pele Principles, underscored by promotion of freedom and opportunity for all its citizens:

1. **Consultation:** Citizens should be consulted about the level and quality of the public services they receive and, wherever possible, should be given a choice about the services that are offered.
2. **Service Standards:** Citizens should be informed of the level and quality of public services they will receive so that they are aware of what to expect.
3. **Access:** All citizens should have equal access to the services to which they are entitled.
4. **Courtesy:** Citizens should be treated with courtesy and consideration.
5. **Information:** Citizens should be given full, accurate information about the public services they are entitled to receive.
6. **Openness and transparency:** Citizens should be informed on how national and provincial departments are run, how much they cost, and who is in charge.
7. **Redress:** If the promised standard of service is not delivered, citizens should be offered an apology, a full explanation, and a speedy and effective remedy; additionally, when the complaints are made, citizens should receive a sympathetic, positive response.
8. **Value for Money:** Public services should be provided economically and efficiently in order to give citizens the best possible value for money.

Further to these, the Municipality has committed to improving efficiency and effectiveness in the manner in which it delivers services to its citizens, which includes the manner through which it administers its daily activities.

The Municipality has further identified ICT as an enabler to the delivery of the IDP delivering on its mandate. In 2015, the Department of Co-operative Governance issued a circular guiding municipalities on the adoption of a Municipal Corporative Governance of ICT Framework, which the municipality has subsequently adopted. Through the adoption of this governance framework, the municipality has further established an ICT steering committee and the adopted policies as mandated by COGTA as formally accepted policies and associated frameworks. The adopted policies may be referenced via *Addendum 1* accompanying this document.

This Strategic ICT Plan therefore seeks to enhance the maturity of the municipalities ICT environment through identifying key initiatives to be delivered by the municipality's ICT environment. These Initiatives have been identified as strategic enablers to the IDP. As such these initiatives, will find its delivery through an ICT architecture roadmap and implementation plan, which will be delivered over a five (5) year cycle, however should be reviewed annually to ensure efficacy.

Furthermore, this ICT Strategy was developed to guide the municipality in delivering upon the *operational plans, work effort* coupled with *capability* planning, as well as *budget estimation(s)* required to deliver upon the key initiatives as outlined towards meeting of the municipality's ICT objectives.

4 Legislation Framework

The Municipality must be aware of and comply with the legislative landscape applicable to their context. Therefore, this strategy was developed with the legislative environment in mind, as well as to leverage internationally recognized ICT standards.

The following legislation, among others, were considered in the drafting of this strategy:

1. Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
2. Copyright Act, Act No. 98 of 1978.
3. Electronic Communications and Transactions Act, Act No. 25 of 2002.
4. Minimum Information Security Standards, as approved by Cabinet in 1996.
5. Municipal Finance Management Act, Act No. 56 of 2003.
6. Municipal Structures Act, Act No. 117 of 1998.
7. Municipal Systems Act, Act No. 32, of 2000.
8. National Archives and Record Service of South Africa Act, Act No. 43 of 1996.
9. Promotion of Access to Information Act, Act No. 2 of 2000.
10. Protection of Personal Information Act, Act No. 4 of 2013.
11. Regulation of Interception of Communications Act, Act No. 70 of 2002.
12. Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.
13. Public Administration Management Act, 2016.
14. Minimum Interoperability Standards (MIOS) for Government Information ***Systems***, 2011.

The following internationally recognized ICT standards were leveraged in the development of this strategy:

1. Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014.
2. COBIT, 2012.

3. ITIL, 2011.
4. International Organization for Standardization (ISO 38500 - Governance of IT), 2015.
5. King IV Report, 2016.

5 Introduction

This document is custom to the municipality and seeks to speak to the ICT landscape; related to both the existing environment and its intended future environment during the course of this lifecycle, as well as alignment to specific initiatives as identified through the preceding sections.

Through strategic alignment, architecture & governance, ICT portfolio assessment, a roadmap and considered annexures for notation as elements or sub-elements – this document serves to both be an ICT analysis asset and simultaneously be set as a *driver of change* through articulation of all items towards consideration.

The workflow of this document is set to identify both caveats and variables towards processes and procedures governing the identified objectives, through which it would seek conclusion of the objectives via operational delivery of all identified items.

This document is specific towards ensuring that the following two (2) overarching and core objectives are met through all the variables delineated on in all preceding sections:

1. As a primary, set towards formulation of a unique *ICT Strategy* for the municipality, through which this document is set towards it as a springboard in terms of guidance of municipal stakeholders.
2. As a secondary, set towards identification of a five (5) year *Implementation Plan* through which all items within the context of this document shall identify all components towards successful governance and management of all initiatives.
3. Note: This document shall additionally be reviewed on an annual basis throughout the duration of the lifecycle of this document. It will also be reviewed in conjunction with the annual IDP review process.

Furthermore, it shall provide context and sentiment towards:

4. Architecture and governance related to policy, procedural and operational considerations.
5. Strategic alignment of both ICT and IDP initiatives.
6. Providing insight and review of existing ICT environment and portfolio.
7. Highlighting of key initiatives with holistic insight into all variables and considerations into actualization.
8. Establishment of various sub-element ICT strategies with a focus on; innovation, e-Governance strategy, service delivery and product sourcing.
9. Value measurement and monitoring.

6 Architecture and Governance

The architecture set in place for steering and guidance of ICT strategy either via frameworks, methodologies or taxonomies are noted as being established from:

1. Control Objectives for Information Technology (COBIT).
2. The Information Technology Infrastructure Library (ITIL).
3. International Organization for Standardization (ISO 38500).
4. The Open Group Architecture Framework (TOGAF).
5. The Zachman Framework (ZACHMAN).

Furthermore, governance adoption or consideration has been identified as:

6. Corporate Governance of ICT Policy Framework (CGICTPF).

7. Corporate Governance of ICT (CGICT).
8. Governance of ICT (GICT).
9. The King IV Report and Code on Governance for South Africa (King IV).
10. Municipal ICT Governance Policy Framework (MICTGPF).

Note: We will not discuss in detail any specifics around governance adoption due to it being too expansive and this document is set within conformance and consideration of all required and governed standards.

The various phases through which critical project or delivery processes are managed shall conform to the above as standard, with key items identified from them in regard to a custom EA framework being set forth towards the endeavour of this ICT *strategy* and its associated *implementation plan(s).*

Therefore, due to this document being drafted for the layman in terms of both understanding and completing of it; specific methodologies will be prescribed through primary concepts for use and consideration. These prescriptions shall be unpacked in simple format to ensure it is adequately and easily understood so that stakeholders without any formal knowledge around EA may easily assimilate the narrative and populate this document accordingly and set forth its use as process to conclude alignment of the strategy, initiatives and/or objectives, where after it will govern capability to embark on a successful orchestration process.

6.1 Contributors to the successful Design, Delivery and Implementation of the ICT Strategy.

Due to the complexity and expansive sets of tools, assets, standards and/or reference models available through various types of Enterprise Architecture (EA), below please find an overview of the components governing this document's framework and its primary contributing factor(s) towards this strategy:

1. COBIT: Provides 210 control objectives applied to 34 high-level IT processes, categorized in four (4) domains: (a) Planning and Organization, (b) Acquisition and Implementation, (c) Delivery and Support, and (d) Monitoring. COBIT recommendations include issues related to ensuring effectiveness and value of IT as well as information security and process governance.
2. ITIL: Provides recommendations for a wide range of IT operations and service delivery best practices including security management and can be mapped accordingly alongside other methodologies to assist in a more expansive holistic framework.
3. ISO/IEC 38500: Provides guiding of a structure of principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of IT within their organizations.
4. TOGAF: Although called a framework, it is more accurately a process toolkit for providing an approach relating to designing, planning, implementing, and governing an enterprise IT architecture through a high-level approach to design. It is typically modelled at four (4) levels: (a) Business, (b) Application, (c) Data, and (d) Technology. It has specific dependencies around modularization, standardization, and already existing, proven technologies and products. Essentially TOGAF is not a step-by-step methodology, but provides an ADM through which stakeholders may develop architecture to meet the business and ICT needs.
5. ZACHMAN: Noted as an EA framework, yet is actually an ontology (branch of items) or taxonomy (scheme of classification) and provides a formal and structured way of viewing and defining an enterprise. It embodies a two (2) dimensional classification schema that reflects the intersection between two classifications. The primary is noted as interrogatives as the business targets, while the secondary is noted as the viewpoints through provisioning or identification of business artefacts.

Therefore, it provides six different transformations of an abstract idea (not increasing in detail, but transforming) from six different perspectives.

All of the aforementioned primaries hold principles for consideration towards the EA framework of this document. Essentially towards the objectives of this document, it may be noted as building a house; ISO/IEC 38500 is set as the roof with its top down interpretation, COBIT could be seen as the walls holding up the structure through applying various controls best suitable, ITIL as a foundation through its best practices, while TOGAF and ZACHMAN being the architects who built/designed the house and thereafter living within it. Therefore, the primaries are essentially piecing of the correct components together to provide longevity as the key component, which will be identified in extended sections and sub-sections below.

6.2 COBIT and ITIL Mapping

The considerations below have been identified as a toolkit in regards to the primary components which large municipalities and departments conform to. The best practices towards the intention of this document has been structured below, with further context provided via an *Addendum 2* accompanying this document.

The various municipal stakeholders towards the strategy, implementation plan(s) and/or initiatives may use the mapping below as guidance towards further or extended value creation. It caters towards specific COBIT library components being translated into *Key Areas* for value creation, which is then mapped to ITIL. Thus, consolidating all the variables and identifying all elements, from process to policy to governance.

Determine Technological Direction
The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems, staffing and investments, as well as improved interoperability of platforms and applications.
Manage the IT Investment
A framework is established and maintained to manage IT-enabled investment programmes that encompasses cost, benefits, prioritization within budget, a formal budgeting process and management against the budget. Stakeholders are consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between IT and business stakeholders; enables the effective and efficient use of IT resources; and provides transparency and accountability into the total cost of ownership (TCO), the realization of business benefits and the ROI of IT-enabled investments.
Manage Human Resources
A competent workforce is acquired and maintained for the creation and delivery of IT services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.
Acquire and Maintain Technology Infrastructure
Organizations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.
Enable Operation and Use
Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.

Manage Changes
All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, and system and service parameters) are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.
Define and Manage Service Levels
Effective communication between IT management and business customers regarding services required is enabled by a documented definition of an agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.
Manage Third-party Services
The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements, therefore needing an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.
Ensure Continuous Service
The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.
Educate and Train Users
Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training programme increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls, such as user security measures.
Manage Service Desk and Incidents
Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.
Manage Operations
Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.

Table 1: COBIT to ITIL Mapping.

6.3 Architecture & Framework Mapping

The Enterprise Architecture (EA) Frameworks that have been considered towards the development of this strategy, are the TOGAF and ZACHMAN frameworks. A high-level overview of these frameworks are covered in the *Addendum 3* accompanying this document. Should the municipality feel that a robust EA is required as part of this strategy, the municipality will be required to capacitate itself accordingly.

7 Benefits Realization Framework

It is required that a Benefits Realization Management (BRM) Framework needs to be established to manage the realization of benefits that this strategy seeks to achieve.

For more particulars related to utilization of BRM, please refer to *Addendum 5* accompanying this document. As an overview, the BRM will take the stakeholder(s) through the processes covering five (5) areas of consideration, as noted below:

1. Define benefits management plan.
2. Identify and structure benefits.
3. Plan benefits realization.
4. Implement change.
5. Realize benefits.

8 Business Challenges Mapping

It is important that all challenges related to the effective and efficient functioning of ICT within the municipality are considered and dealt with appropriately.

For specifics towards managing expectations around the challenges of the municipality, please review *Addendum 4* accompanying this document for guidance on handling of challenges.

9 ICT Strategic Alignment

The intent throughout the document is to align the municipal IDP with the ICT Strategy and this section deals with the elements of the ICT strategy and its alignment with the IDP.

There will be a number of ICT initiatives that have will need to be identified by the municipality for alignment towards meeting the specific or predefined IDP initiatives set as the table below. This table is solely noted as a high-level overview as a summary, with more detail around it provided in the sections below – it is here as the core item to this section, to provide a consolidated view around the initiatives, as born through the IDP objectives.

ICT Initatives 2017 - 2022 (15)	
1.	End User Computer Refresh
2.	Implement Public WiFi Service
3.	Develop Public Engagement App.
4.	Implement CCTV with analytics
5.	Enhance system and network security
6.	Establish a fully functional Desktop Support Services
7.	Upgrade / roll out Access Control
8.	Implement Mail Archiving solution
9.	Upgrade ICT Disaster Recovery capabilities
10.	Implement Disaster Reovery plan
11.	Establishing and implementing Intranet
12.	Upgrading of Wide Area Network (WAN)
13.	Upgrading of Local area network (LAN)
14.	Upgrade Internet Connectivity
15.	Develop an ICT Maintenance plan

IDP Objective 2017 - 2022 (12)	
1.	To create a culture of good governance
2.	To create a culture of public participation and empower communities to participate in the affairs of the Municipality
3.	To create an administration capable of delivering on service excellence.
4.	To create an enabling environment for economic growth and development
5.	To promote tourism in the Municipal Area
6.	To provide effective financial, asset and procurement management
7.	Provision of equitable quality basic services to all households
8.	To maintain infrastructure and undertake development of bulk infrastructure to ensure sustainable service delivery.
9.	To provide community facilities and services
10.	Development of sustainable vibrant human settlements
11.	To promote social and youth development
12.	To create and maintain a safe and healthy environment

Table 2: ICT and IDP Alignment.

9.1 Municipal ICT Vision Statement

Deliver Municipal and community focused ICT products and services that are effective, secure, supportive and conducive of the vision of Cape Agulhas Municipality.

9.2 Municipal ICT Mission Statement

The mission are to focus on closing the gaps identified and using the opportunities that exist to strategically position Cape Agulhas Municipality to better deal with the issues and needs affecting the Information users and communities, how best to use ICT to speed up municipal strategic goals and assist in the realize of IDP objectives in order to create a safer environment that will promote socio-economic growth and ensure future financial sustainability in a prosperous southernmost community.

9.3 ICT Stakeholder Map

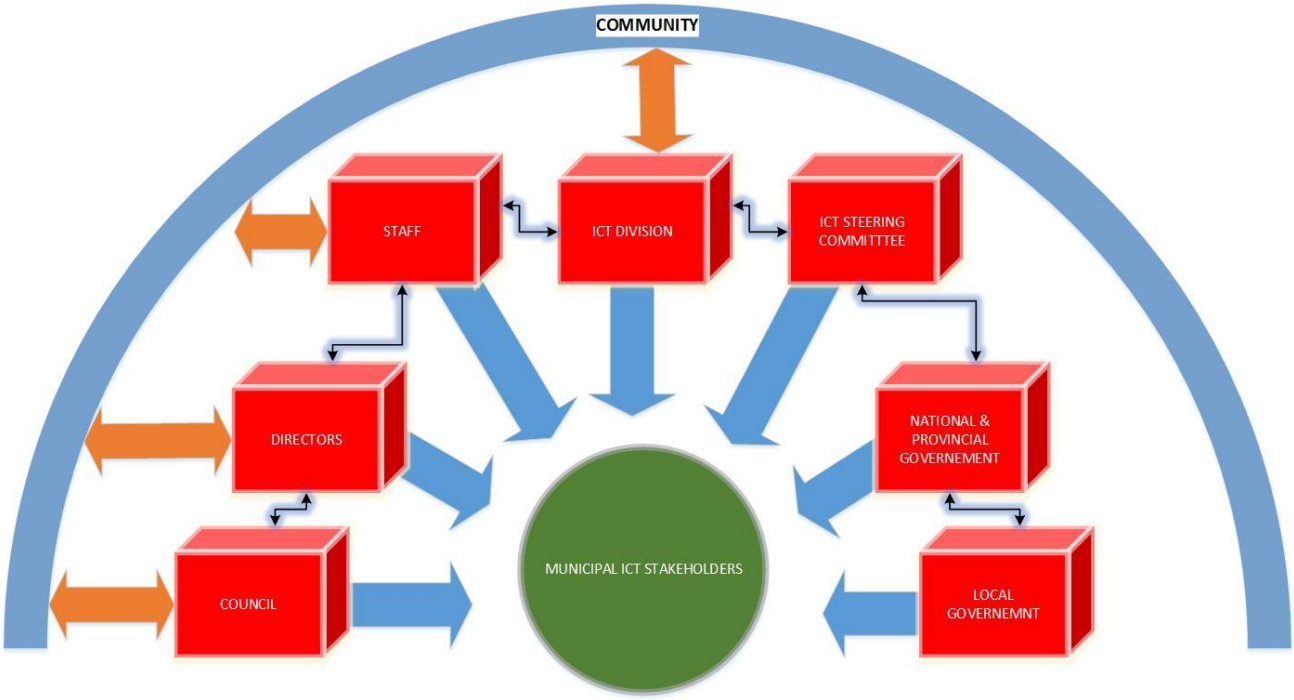

Figure 4: Structure – ICT stakeholder map

9.4 ICT Departmental Objectives

Objectives are defined by the municipality as identified either by the IDP, the department(s), or its stakeholders, through which initiatives are identified towards meeting of the objectives.

Therefore, through the sections below we shall aim for:

1. Understanding of the objectives.
2. Clearly identify initiatives, with intended details around project.
3. Obtaining of details around the background and history of the objective and/or initiative.
4. Identify details around the objective/initiative as per predefined sub-sections below within this section.
5. Compilation of a full breakdown-structure related to the required, proposed or intended budget(s).

To note that through this aim we will understand each item within its entirety, with its intended and associated implementation plan(s) being specified as a high-level view in the preceding section as within the roadmap.

9.4.1 Initiatives and Business Case

This section delineates on each of the departments ICT objectives from a top-down structure. Cases through which initiatives are born are then set into their own independent sub-section, to obtain the full business case of each item towards its entirety and be held in a separately and easily referenceable section.

In essence, this section embodies several subsections, each articulating everything holistically towards each initiative.

It is important to note that each Business Case as identified below will be linked to a specific IDP Project as identified in the Municipal Standard Charter of Accounts (mSCOA).

9.4.1.1 Business Case 1: ICT Governance

ICT Governance encompasses various structures, roles and responsibilities that can be utilized, managed and controlled with the assistance of mechanisms to achieve this.

The challenge for the Municipality is therefore to determine which of these mechanisms can be used and how to successfully deploy these, in order to achieve the set strategic mission and vision of this organization.

With this in mind, the intention is to determine key points that can help to identify these mechanisms and can be defined as follows:

- Strengthen the ICT institutional framework and internal policy
- ICT Audit Trails, logging and Activity Reports
- Database Administration and ICT Change Controls
- Third Party Management
- Risk Management

9.4.1.1.1 Strengthen the ICT institutional framework and internal policy

Studies have shown that institutional framework has a strong influence on the extent, adequacy, accuracy and speed of delivering information services. The effective use of ICT remains the only feasible way of controlling and maintaining vast amounts of information required to efficiently and effectively operate an organization.

As this positively affects the growth of economies, CAM should deploy ICT and make them the cornerstone upon which municipal services and functions are built.

The institutional framework of CAM is very deficient. The major challenge that the Municipality were faced with in the past were the lack of an internal structure such as an ICT Department or Municipal ICT Committee mandated to oversee the development and establishment of ICT applications and services. This however were partially attended to, as an ICT Steering Committee has been established.

There is no ICT strategy. The establishment of an ICT department responsible for general development, maintenance and oversight of ICT infrastructure and services and the setting-up of an ICT Committee in the Municipality to support the role of the Municipality and oversee implementation of the ICT Master Plan or Strategy should enhance the institutions ability to deal with demands and challenges emanating from its stakeholders.

In general, the ICT Committee could oversee ICT projects and ensure a conducive and enabling environment for effective ICT awareness, implementation, access, usage, policy formulation and budget.

At the policy level, awareness of ICT potentials should be a heightened and strategic thinking and planning to systematically deploy ICTs increased with a view to adequately using these potentials and fully reaping from them.

Given the absence of an ICT Department in the CAM, the forming of such a department was approved to in accordance with the internal rules of the Municipality and officially opened in August 2014. We found a need to establish an ICT Department with an ICT Strategic Plan that would clearly take into account the Vision and Mission of the Municipality.

Outlines guiding principles for a Municipal Information System Management to provide reliable, secure, useful, and easily-accessible information resources, information for general use, ownership, security and proprietary information, unacceptable use, system and network activities, emails, budgeting and resource mobilization mechanisms and communication activities as well as to ensure implementation must be developed. Each Director and employee should take responsibility for the accuracy, timeliness, protection and preservation of information resources within the Municipality. This principles will include the following components:

a. Municipal ICT Organogram;

b. The ICT Committee;

c. Responsibilities/functions;

d. The Information system guiding principles, usage and access; and

e. Security and Privacy: The Master Plan should ensure:

i) Data is protected;

ii) Users are authenticated;

iii) Data confidentiality and integrity are preserved; and

iv) Non-repudiation is achieved.

1. The maintenance plan:

i) Hardware maintenance by making available parts and back-up equipment; and

ii) Software with vendor support (on-site/off-site) to fix bugs/resolve problems, helpdesk support, scalability and support for system software upgrades.

2. Business continuity plan: enables critical services or products to be continually delivered to stakeholders.

3. Budgeting/Resource mobilisation processing: developing a proper cost-benefit analysis to identify resource needs and propose a different innovative resource mobilisation strategy, including local year

budget allocation, private sector involvement, bilateral and multilateral participation and Diaspora participation.

4. *Monitoring and evaluation mechanism: To monitor cost-effectiveness, impacts, progress in the use of ICT in administration and municipal functions, learning and research, and to provide management information to empower Departments and the Municipality as a whole.*

5. *Risk assessment.*

9.4.1.1.2 ICT Audit Trails, logging and Activity Reports

Before we begin, there is a very important caveat to bear in mind - log data doesn't help if it isn't reviewed! As today's systems are often generating thousands of lines of data per day, if not per hour, manual review isn't very realistic. Log centralization and analysis tools should be used to automatically alert on certain conditions as well as help facilitate meaningful log review.

Event data should be logged on a given system if the business need requires it. Essentially there are four categories of reasons:

- Accountability – Log data can identify what accounts are associated with certain events. This information then can be used to highlight where training and/or disciplinary actions are needed.

- Reconstruction – Log data can be reviewed chronologically to determine what was happening both before and during an event. For this to happen, the accuracy and coordination of system clocks are critical. To accurately trace activity, clocks need to be regularly synchronized to a central source to ensure that the date/time stamps are in synch.

- Intrusion Detection – Unusual or unauthorized events can be detected through the review of log data, assuming that the correct data is being logged and reviewed. The definition of what constitutes unusual activity varies, but can include failed login attempts, login attempts outside of designated schedules, locked accounts, port sweeps, network activity levels, memory utilization, key file/data access, etc.

- Problem Detection – In the same way that log data can be used to identify security events, it can be used to identify problems that need to be addressed. For example, investigating causal factors of failed jobs, resource utilization, trending and so on.

Security of Logs

For the log data to be useful, it must be secured from unauthorized access and integrity problems. This means there should be proper segregation of duties between those who administer system/network accounts and those who can access the log data.

The idea is to not have someone who can do both or else the risk, real or perceived, is that an account can be created for malicious purposes, activity performed, the account deleted and then the logs altered to not show what happened. Bottom-line, access to the logs must be restricted to ensure their integrity. This necessitates access controls as well as the use of hardened systems.

Consideration must be given to the location of the logs as well – moving logs to a central spot or at least off the sample platform can give added security in the event that a given platform fails or is compromised.

Audit logs are beneficial to have for a number of reasons. To be effective, IT must understand log requirements for each system, then document what will be logged for each system and get management's approval. This will reduce ambiguity over the details of logging and facilitate proper management.

These logs are governed by means of the ICT Policies of Cape Agulhas Municipality.

9.4.1.1.3 Database Administration and ICT Change Controls

Database administration refers to the whole set of activities performed by a database administrator to ensure that a database is always available as needed. Other closely related tasks and roles are database security, database monitoring and troubleshooting, and planning for future growth.

Database administration is an important function in any organization that is dependent on one or more databases.

It is important that the relevant System Administrator of the various MIS`s are well trained and/or supported by means of a Service Level Agreement in order to fully understand importance and maintain the various Databases residing in these Municipal Information Systems.

The integrity of the data as well as the manner in which employees gain access to the information to these databases are of the utmost importance as it directly affect information provided to Management of decision making and service delivery in the Municipal area.

Controls put in place need to be enforced to ensure the validly and integrity of the data and has to run hand in hand with audit trails and logs being kept for the respective MIS and change control measures has to be in place in order to manage any change in a MIS that can by any means affect the use of the system or the integrity of the respective database.

Therefore a formal approved Change Control Process has to be in place to ensure that all changes made are logged and approved in terms of the ICT Governance regulations.

9.4.1.1.4 Third Party Management

Third parties are defined as anyone not employed directly by CAM`s Council and includes partners such as other local authorities, as well as suppliers who require access to the council's network. All entities supplying a MIS or ICT service are considered third parties for the purposes of network and data access.

Third Parties are individuals and organisations which fall into the following categories. These will include, but not be limited to:

Contracted staff

a) Hardware and software maintenance and support staff

b) Temps and agency staff that are not employed by Cape Agulhas Municipality

Third Parties requiring administrative access to council systems

c) External IT support staff

d) Suppliers (including Suppliers of IT goods, systems or services)

e) Auditors not employed directly by the council

A valid proses or policy has to be drafted, approved and documented in order to ensure how the Municipality deal with third parties.

It is also of the utmost importance that a valid SLA has to be in place, stipulating the responsibility of all stakeholders related to these agreements and should a third party require access to the network of the Municipality how, where, when and under what circumstances they should be authorized to gain access to the network.

9.4.1.1.5 Risk Management

The **ICT risk management** is the application of risk management to Information technology context in order to manage IT risk.

IT risk management should be considered a component of a wider enterprise risk management system.

A formal risk assessment process has been done by CAM whereby ICT risk in the broader spectrum of the Municipality has been included.

A detailed risk register concerning ICT Risks has also been developed, based on ISO 27K standards and should be reviewed annually and as new risks occur or are identified.

Scope of Work (SOW) related to ICT initiatives

- Develop Public Engagement Application (App)
- Establish a fully functional Desktop Support Service
- Implement a Mail Archiving Solution
- Establish and implement an Intranet
- Develop an ICT Maintenance Plan

Benefits related to ICT initiatives

- Enhance Public participation
- Enhance fault reporting and response times
- Value for money
- Knowledge sharing internal and external to Municipality
- Functional systems and services

Risks related to ICT initiatives

- Preventative maintenance not done diligently
- Loss of key dependencies
- Loss of knowledge
- Reputation risk

Note: Risks will be managed in accordance to the risk management policy of the municipality around ICT.

Through the above items, points and/or considerations as context; the ICT initiative below has been identified:

1.	Develop Public Engagement App. set as a driver towards Creating a culture of public participation and empower Communities to participate in the affairs of the Municipality, to improve tourism in the Municipal Area and to provide community facilities and services	IDP Reference	SO. 2 SO. 5 SO. 9

Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	**Q1**	**Q2**	**Q3**	**Q4**	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Champion(s):	Chief Information Officer																		
Department:	Finance					**Completion by:**		2020/Q4				**Priority:**				L	**M**	H	
Associated Costs:	Q1: R0 .00	C	O	Q2: R 0.00	C	O	Q3: R 0.00	C	O	Q4: R 200 000	**C**	O							
Total Project Value:	R 200 000			**Total CAPEX:**	R 200 000			**Total OPEX:**	R 0.00										
Budget (Funded):	R 0. 00			**Unfunded:**	R 200 000			**Short:**	R 200 000										

Table 3: Objectives, Initiative and Business Case.

2.	*Establish a fully functional Desktop Support Service* set as a driver towards creating a culture of good governance	IDP Reference	SO. 1

Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	**Q1**	**Q2**	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Champion(s):	Chief Information Officer																		
Department:	Finance				**Completion by:**			2019/Q4 ongoing			**Priority:**			L	M	**H**			
Associated Costs:	Q1: R 72 500	C	**O**	Q2: R 72 500	C	**O**	Q3: R 72 500	C	**O**	Q4: R 72 500	C	**O**							
Total Project Value:	R 1 160 000			**Total CAPEX:**	**R 0.00**		**Total OPEX:**	**R 1 160 000**											
Budget (Funded):	R 0.00			**Unfunded:**	R 1 160 000		**Short:**	R 1 160 000											

Table 4: Objectives, Initiative and Business Case.

3.	Implement Mail Archiving Solution set as a driver towards creating a culture of Good Governance, and to create an administration capable of delivering on service excellence	IDP Reference	SO. 1 SO. 3

Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	**Q1**	**Q2**	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Champion(s):	Chief Information Officer																		
Department:	Finance				**Completion by:**			2018/Q2			**Priority:**			L	M	**H**			
Associated Costs:	Q1: R 0.00	C	O	Q2: 250 000	**C**	O	Q3: R 0.00	C	O	Q4: R 0.00	C	O							
Total Project Value:	R 250 000			**Total CAPEX:**	R 250 000		**Total OPEX:**	R 0. 00											
Budget (Funded):	R 200 000			**Unfunded:**	R 50 000		**Short:**	R 50 000											

Table 5: Objectives, Initiative and Business Case.

4.	Establishing and implementing an Intranet set as a driver towards creating an administration capable of delivering on service excellence.	IDP Reference	SO. 3

Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	Q1	Q2	Q3	**Q4**	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Champion(s):	Chief Information Officer																		
Department:	Finance				**Completion by:**			2018/Q4			**Priority:**			**L**	M	H			
Associated Costs:	Q1: R 0.00	C	O	Q2: R 0.00	C	O	Q3: R 0.00	C	O	Q4: R 50 000	C	**O**							
Total Project Value:	R 50 000			**Total CAPEX:**	R 0.00		**Total OPEX:**	R 50 000											
Budget (Funded):	R 50 000			**Unfunded:**	R 0.00		**Short:**	R 0.00											

Table 6: Objectives, Initiative and Business Case.

5.				Develop an ICT Maintenance plan								IDP Reference				N/A			
Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):				Chief Information Officer															
Department:				Finance				Completion by:				2018/Q4			Priority:			L	M	H
Associated Costs:				Q1: R 0.00		C	O	Q2: R 0.00		C	O	Q3: R 60 000		C	O	Q4: R 60 000		C	O
Total Project Value:				R 120 000				Total CAPEX:				R 0.00			Total OPEX:			R 120 000	
Budget (Funded):				R 0.00				Unfunded:				R 120 000				Short:		R 120 000	

Table 7: Objectives, Initiative and Business Case.

9.4.1.2 Business Case 2: ICT Infrastructure – Strengthening ICT Infrastructure

It is practically impossible to exploit opportunities offered by ICT and reap the corresponding benefits without appropriate technical infrastructure to provide the platform for access and delivery of applications and services.

Municipal infrastructure should be maintained in a condition that would facilitate communication and/ or information exchange, enhance the objectives of the municipality functions of legislation, representation oversight and optimally managing the knowledge capital and human resources, whenever the need arises. This would enable the Municipality to ensure regular maintenance and upgrading, adopt professional security measures to provide adequate ICT support and services and that internal operations need to be sustained.

Cape Agulhas Municipalities ICT infrastructure consist mainly of desktop computers, laptops, security equipment, printers, photocopiers, scanners, a LAN and restricted Internet connection, leased lines from Telkom and wireless infrastructure, supplied and managed by a Service Provider.

Human resources play a vital part in the municipal functions and values. Hence, the need to develop strategies for strengthening and increasing work force quantity and quality and ICT skills-based personnel to convert ICT knowledge and skills into services for the benefit of Municipality and its community.

The ICT Strategic Plan development has three activities as illustrated in the below.

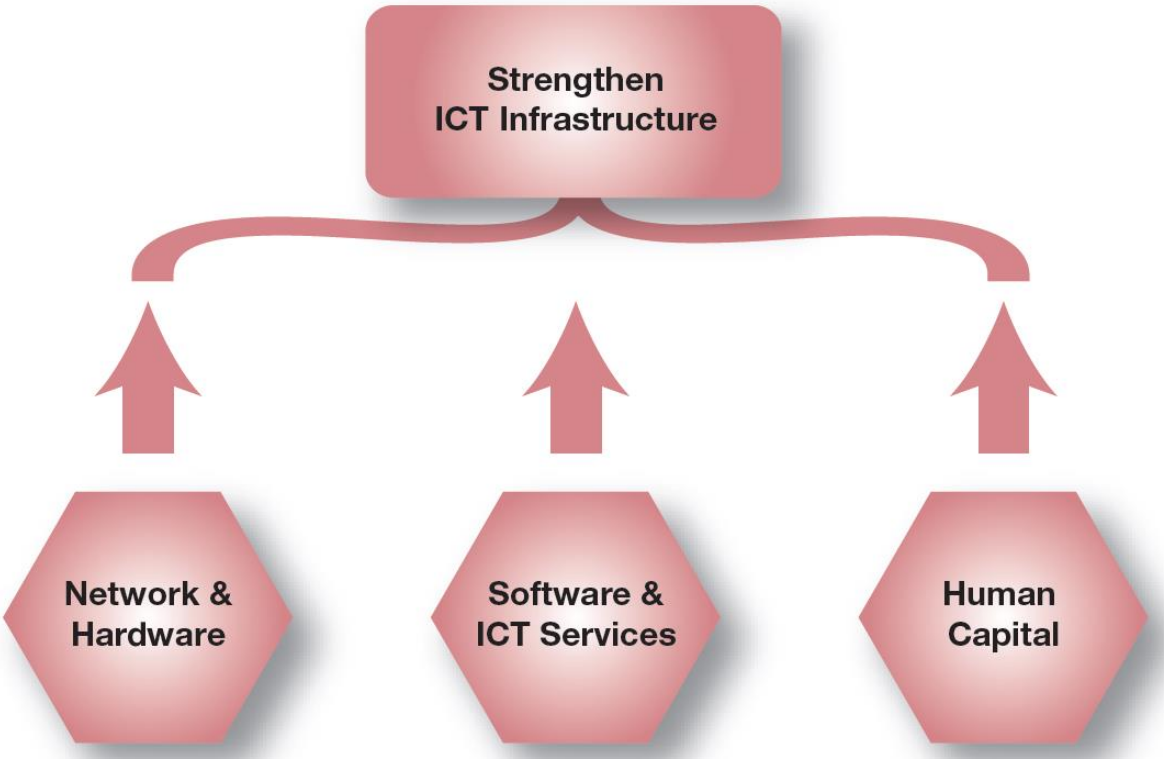

Figure 5: Structure – Strengthening ICT Infrastructure

With the aforementioned in mind, this infrastructure will be defined in the following sections with each consisting of its own subsections:

- To strengthen Network and Hardware Infrastructure
- To Improve Software and ICT Services
- Human Capital Infrastructure

9.4.1.2.1 To strengthen Network and Hardware Infrastructure

The main objective here is to strengthen and improve the physical connections of all networks in meeting rooms, Council Chambers and offices at the Municipality - servers, bandwidth capacity, wireless access, network security and associated hardware.

The level of network and hardware infrastructure are not adequate in the Municipality. The infrastructure in its current state cannot adequately service the internal demands of the Municipality.

Although steps has been implemented to address the issue at hand there are still quite a few sites and Municipal buildings that has insufficient or redundant network connection to the Data Centre of the Municipality.

Establishment of ICT infrastructure facilities and services are no longer an option but a necessity in order to meet both internal and external demands of stakeholders. The Municipality is committed to facilitating

connectivity to all of its Sites and buildings and to ensure adequate stable and reliable connectivity to these sites and buildings ensure cost-effective service delivery.

Focus areas include:

1. Increasing network bandwidth, connectivity and Internet bandwidth.
2. Upgrading of existing older networks at respective sites and offices – LAN and interconnection - CAT, Fibre, Wireless.
3. Increasing server capabilities and increasing VM environment relating to storage and storage solutions. –information and knowledge repository servers and print server.
4. Availing of the heavy-duty facilities like printing and photocopying.
5. Upgrading older and redundant computers and laptops
6. Upgrading of Server room
7. Upgrading of Disaster Recovery (DR) Site
8. Access control and security – cameras, alarms etc.

9.4.1.2.2 Local Area Network (LAN) and Wide Area Network (WAN)

The LAN, connects about sixty (60) offices at the Head Office at Bredasdorp, six (6) offices at Bredasdorp Stores, ten (10) offices at Bredasdorp Traffic Department, seven (7) offices at the Thusong Centre Bredasdorp, one (1) offices at Struisbaai Campsite, eight (8) offices at Struisbaai Head Office, two (2) offices at L`Agulhas Campsite, one (1) office at Arniston Campsite and six (6) offices at Napier Office that consist of mainly officials in the various Municipal buildings. The Purpose of this LAN is to facilitate access to essential centrally provided services, like Internet, emails and other relevant Municipal Information Systems. This service could be expanded, monitored and managed to provide enhanced ICT services to the all staff members. Video conferencing facility is not available. All approved end users has access internet connection.

The WAN, connects twenty one (26) sites that include the above mentioned LAN sites as well as other Municipal supported sites such as libraries, sewage plants and water purification plants.

9.4.1.2.3 Broadcasting and Infrastructure

CAM does not currently provide Broadband services to its residence but should strive to cooperate with its neighbour Municipalities and Provincial government in terms of the Broadband initiative of the Western Cape Government. This tender has been awarded to Neotel in 2014 and its main purpose is to connect all individuals of the Western Cape Province.

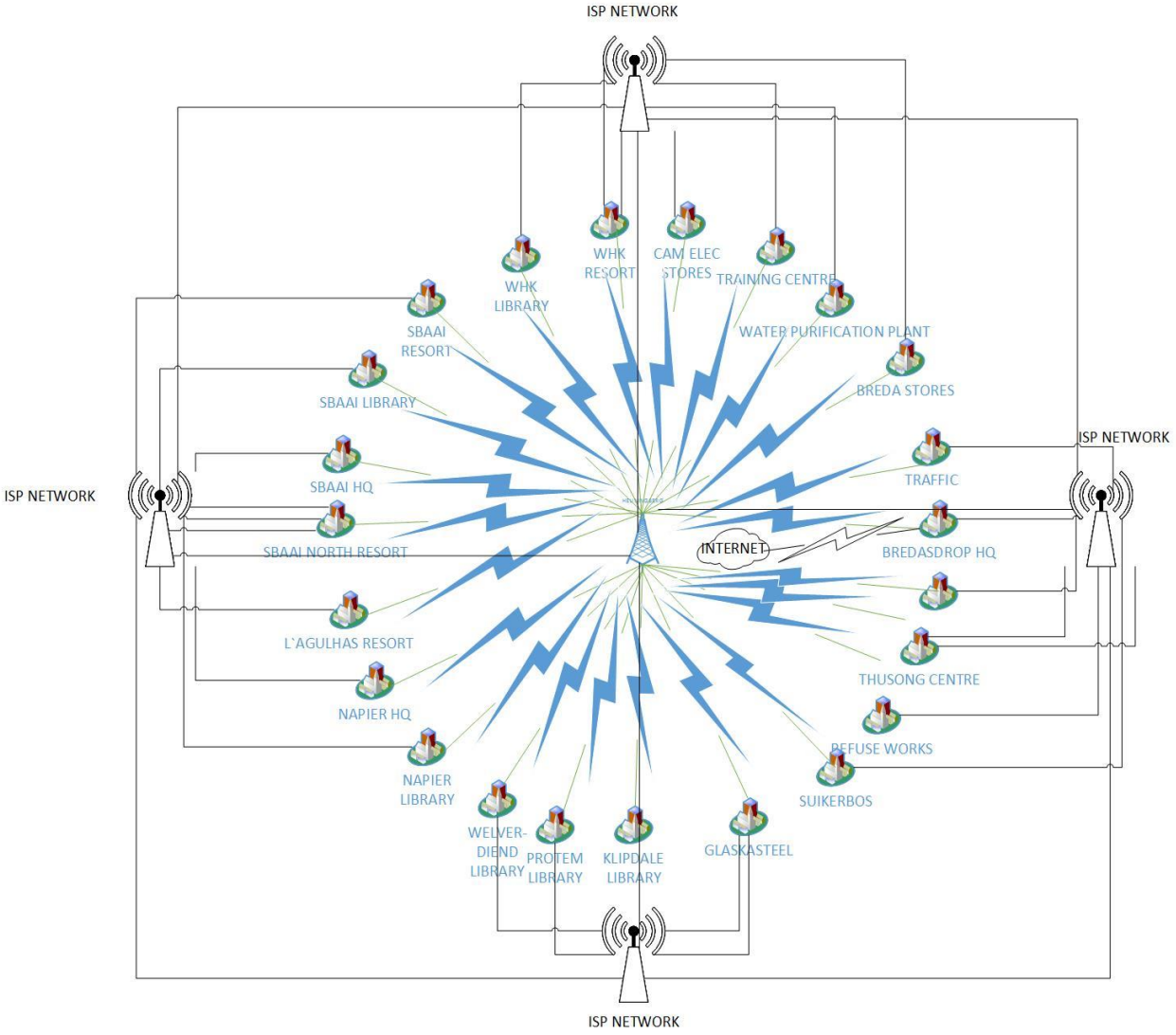

Figure 6: Virtual private Network Overview

9.4.1.2.4 To Improve Software and ICT Services

The objective of this section is to improve the tools and applications used by Staff of the Municipality to perform their functions, by addressing the challenges, inadequacies and weaknesses. Some of the major challenges for officials are the lack of awareness of the opportunities and benefits of ICT deployment and inadequate computer training, which limits proper use of the available ICT resources resulting in lack of integration of ICT services and applications into office work.

9.4.1.2.5 Applications software

In terms of application software officials use MS Office for general purpose applications and most of the specialized applications in terms of MIS`s are available for Municipal use. Although some third party software are available and been utilized by officials there may still be some short falls relating to some job functions.

Website Design

The Municipalities webpage, although outsourced, has been upgraded to a highly interactive website with online forums and blogs, incorporating themes on the vision, mission and functions of the Municipality, with relevant content that addresses the information needs of employees and Ratepayers. This however does not mean that the website would not require periodic updating by relevant qualified staff.

The Municipality may consider the need to train or employ officials to perform this function in house.

The Municipality should consider acquiring the following services as they are currently not available.

Intranet

Information availability are at the heart of the Municipality and by implementing an Intranet within the Municipality information and resource sharing can greatly enhance service delivery and promote financial viability.

Help Desk

Increased use of ICT in Municipality would require efficient and effective support to users. This requires equipping ICT services with a help desk software to help manage requests efficiently. Tracking emails and phone calls become easier when requests are managed with several automated processes like request routing and Frequently Asked Questions (FAQ) on the Municipalities intranet.

Mail Archiving

In terms of the National Archive legislation information has to be stored for various periods in time and this also relate to the record keeping or archiving of all correspondence such as emails being generated or received by officials of the Municipality.

To strengthen service delivery, security and legislative requirements, the Municipality should investigate a Mail Archiving system or software.

9.4.1.2.6 ICT Services

ICT are being utilized by various Departments within the Municipality supporting various Municipal Information Systems.

The key to success in the utilization of these various supporting companies lays in the way this support are been managed and evaluated in terms of their performance. The key focus area here also lies in the way training are provided by the supporting companies in enabling the employees and Administrators relative to these various MIS`s, in other words, how transfer of skills are presented in order to empower employees and System Administrators to become less dependent on Service Providers.

Notwithstanding the fact that these ICT Services will never be fully become none and void, but should empower employees to become less dependent on these services to promote better service delivery to the ratepayer and promote financial viability.

Duplication of these services should also be investigated to promote the same principles as previously mentioned.

9.4.1.2.7 Human Capital Infrastructure

An improved human capital infrastructure is essential for the development, management and use of ICT applications and services. One of the greatest challenges in ICT departments has been the lack of skilled and competent staff capable of optimally using ICT applications. In order to improve the quality of ICT governance, the Municipality should focus on developing and implementing innovative strategies for retaining skilled and competent staff.

For the Municipality, the human capital infrastructure when developed would be the technical and administrative support staff.

The majority of staff members had access to ICT services and applications, but sufficient ICT training in 'basics of computer' and 'more computer knowledge' and Internet training should enjoy attention. This calls for systematic and regular capacity building ICT initiatives, especially in view of the rapid changes in the ICT environment.

9.4.1.2.7.1 Municipal Technical staff

As the use of ICT grows, so does the need for regular maintenance of equipment, new software upgrades, implementation of new and better performance technical equipment and the Municipality becoming increasingly dependent upon its technical staff for unimpeded service delivery. Thus, the Municipality must be able to attract and retain good technical support staff by offering attractive conditions of service, regular in-house training and new opportunities for career development.

Although the Municipality have formed an ICT department many ICT services and applications are externally provided, therefore specialized training, linked to specific responsibilities, for staff responsible for ICT operations and ICT applications, respectively should be provided continuously.

9.4.1.2.7.2 Municipal Employees

The use of ICTs not only extends the Municipality to the people but also addresses the challenges of globalization by enabling Employees and Councillors to think beyond their immediate municipal boundaries.

Providing training to employees regarding the various ICT resources available to them, empowers employees to provide better service delivery. The challenge however are to determine which employee require training related to which MIS or ICT tool, without spending money on training not in line with the post the employee resides in.

9.4.1.2.7.3 ICT Committee Members

The Municipalities ICT Committee members are to coordinate and ensure effective implementation of the ICT Strategy Plan. They are essential for lobbying for the deployment and use of ICTs in the Municipality; overseeing ICT projects being undertaken by the IT- and other departments and leading the establishment of

an appropriate enabling environment, including ICT legislative and regulatory frameworks for harnessing the potentials of ICT for socio-economic and Municipal service development.

Therefore, all members of the ICT committee should be given special training and sensitized on all ICT services and policy formulation, implementation and monitoring, including policy development, identification of priority development areas. The financial implications of this special training should be considered.

Well trained ICT Committee members will actively support awareness-raising and capacity- building activities to enhance the capacity of the Municipality to monitor existing policies ensuring that they comply with national standards and developments, lobbying for appropriate ICT policies. This will also enhance Committee member's effective participation in ICT policy formulation, implementation and monitoring for an inclusive, people-cantered and development-oriented knowledge society. They will therefore take an active part and play a leading role in ensuring investment in ICTs by developing strategies that facilitate access to ICTs and information for the Municipality and the whole Cape Agulhas Municipal area.

9.4.1.2.8 Outsourcing of ICT activities

ICT maintenance is done by the ICT Department.

In some instances where high level system or service support are required, this may be outsourced to the relevant MIS provider, as appointed through relevant SCM procedures and that are linked to valid SLA`s and performance evaluation.

9.4.1.2.9 Shared Services & Cooperative Governance

Shared services becoming more and more relevant in Municipal environments around the country, enhances the capabilities of participating Municipalities.

The purpose of this concept are to enhance services, service delivery, economy and social development of communities in the governed areas.

Participating Municipalities has to find a way in which shared services can be implemented to share services such as knowledge sharing, infrastructure procurement, economic development, value for money and better service delivery.

The best platform for this concept are at district level as the Overberg ICT forum.

Scope of Work (SOW) related to ICT initiatives

- End User Computer Refresh
- Implement Public WI-FI Services
- Upgrading of Wide Area Network (WAN)
- Upgrading of Local Area Network (LAN)
- Upgrade Internet Connectivity

Benefits related to ICT initiatives

- Local Economic Development
- Enhancing Service Delivery
- Functioning Staff
- Public Participation
- Informed Communities
- Functional Infrastructure
- Improved Connectivity

Risks related to ICT initiatives

- Loss of Data Services
- Drain on Resources
- Inability to Provide Services
- Client Dissatisfaction
- Loss of Key Dependencies
- Reputational Risk

Note: Risks will be managed in accordance to the risk management policy of the municipality around ICT.

Through the above items, points and/or considerations as context; the ICT initiative below has been identified:

1.	End User Computer refresh set as a driver towards Maintaining infrastructure and undertake development of bulk infrastructure to ensure sustainable service delivery								IDP Reference				SO. 8						
Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Senior ICT Technician																		
Department:	Finance				Completion by:				Ongoing / yearly				Priority:			L	M	H	
Associated Costs:	Q1: R 0. 00		C	O	Q2: R 300 000		C	O	Q3: R 0.00		C	O	Q4: R 0.00			C	O		
Total Project Value:	R 300 000 yearly				Total CAPEX:		R 1 200 000				Total OPEX:		R 0.00						
Budget (Funded):	R 900 000				Unfunded:		R 300 000				Short:		R 300 000						

Table 8: Objectives, Initiative and Business Case.

2.	Implement Public WI-FI Services set as a driver towards creating a culture of public participation and empower communities to participate in the affairs of the Municipality, to create an enabling environment for economic growth and development, to promote tourism in the Municipal Area, to provide community facilities and services and to promote social and youth development			IDP Reference	SO. 2 SO. 4 SO. 5 SO. 9 SO. 11
Year 1 (2017-2018)	Year 2 (2018-2019)	Year 3 (2019-2020)	Year 4 (2020-2021)	Year 5 (2021-2022)	

Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Chief Information Officer																		
Department:	Finance							**Completion by:**	2020/Q4			**Priority:**			L	**M**	H		
Associated Costs:	Q1: R 900 000	C	**O**	Q2: 900 000	C	**O**	Q3: 900 000	C	O	Q4: 900 000	C	**O**							
Total Project Value:	R 7 200 000			**Total CAPEX:**				**Total OPEX:**	R 7 200 000										
Budget (Funded):	R 0.00			**Unfunded:**	R 7 200 000			**Short:**	R 7 200 000										

Table 9: Objectives, Initiative and Business Case.

3.	Upgrading of Wide Area Network (WAN)	IDP Reference	N/A

Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Senior ICT Technician																		
Department:	Finance							**Completion by:**	Ongoing / yearly			**Priority:**			L	M	**H**		
Associated Costs:	Q1: R 90 000 . 00	C	**O**	Q2: R 90 000	C	**O**	Q3: R 90 000	C	**O**	Q4: R 90 000	C	**O**							
Total Project Value:	R 600 000 yearly			**Total CAPEX:**	R 0			**Total OPEX:**	R 3000 000										
Budget (Funded):	R 1 200 000			**Unfunded:**	R 0 .00			**Short:**	R 1 200 000										

Table 10: Objectives, Initiative and Business Case.

4.	Upgrading of Local Area Network (LAN)	IDP Reference	N/A

Year 1 (2017-2018)				Year 2 (2018-2019)				Year 3 (2019-2020)				Year 4 (2020-2021)				Year 5 (2021-2022)			
Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Senior ICT Technician																		
Department:	Finance							**Completion by:**	2019/Q4			**Priority:**			L	M	**H**		
Associated Costs:	Q1: R 0. 00	C	O	Q2: 50 000	**C**	**O**	Q3: R 0.00	C	O	Q4: R 0.00	C	O							
Total Project Value:	R 250 000			**Total CAPEX:**	R 164 000			**Total OPEX:**	R 86 000										
Budget (Funded):	R 100 000			**Unfunded:**	R 150 000			**Short:**	R 150 000										

Table 11: Objectives, Initiative and Business Case.

5.	Upgrading of Internet Connectivity	IDP Reference	N/A

Year 1 (2017-2018)	Year 2 (2018-2019)	Year 3 (2019-2020)	Year 4 (2020-2021)	Year 5 (2021-2022)

Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Senior ICT Technician																		
Department:	Finance							**Completion by:**				2021/Q4				**Priority:**		L	**M** H
Associated Costs:	Q1: R 60 000		C	**O**	Q2: 60 000		C	**O**	Q3: R 60 000		C	**O**	Q4: R 60 000		C	**O**				
Total Project Value:	R 960 000				**Total CAPEX:**	R 0.00				**Total OPEX:**	R 960 000								
Budget (Funded):	R 720 000				**Unfunded:**	R 240 000				**Short:**	R 240 000								

Table 12: Objectives, Initiative and Business Case.

9.4.1.3 Business Case 3: Security Framework

Information and information systems are critical and vitally important to the Municipality. Without reliable information the Municipality could be adversely affected, both financially and reputation wise. Therefore, there are a need to set the minimum requirements and the responsibility that all employees, temporaries, contractors and management must comply with in order to secure the Municipality's information.

Therefore, we have to set out the approach taken to manage information security to ensure that information assets are properly protected against a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accidental.

In order to reach these goals various measures need to be implemented to ensure the security of data, assets, ICT environment and the employees of the Municipality.

9.4.1.3.1 Server rooms

These server rooms, also named data centres consist of any designated area or specific site, containing servers a hosting MIS or a copy thereof that can be accessed in a normal working environment or in a Disaster Recovery or testing capability.

The focus here are to improve and strengthen security measures regarding these sites. This include physical and software related factors such as the hardware environment, software being utilized, physical access control and the monitoring thereof.

The key here is in developing a working document of best practices relating to such an environment that include the concept of technologies, software and environmental controls that need to be in place to ensure that sufficient security are in place to secure the data and integrity of the Municipality and the reputation thereof.

9.4.1.3.2 Security Software

9.4.1.3.2.1 Current security software status

The protection of the data of the Municipality should be one of the key focus areas of any organization. This protection although enforced by physical factors as well, should also be protected by means of software for attacks such as virus, anti-spam and unauthorised access, internally as well as externally.

Although various forms of software relating to this kind of risk are already implemented by the Municipality the ever-changing ICT environment and the skills and knowledge of entities growing at such an immense rate should be taken into consideration as well.

The Municipality implemented two firewalls, securing the network from attacks, firstly from the first ISP providing the VPN and secondly from the internet provided by a secondary ISP for redundancy purposes.

Network protection on the edge of the network is further protected by means of a firewall implemented.

Furthermore each virtual server and end user device, which include both computers and laptops are protected with a third firewalls that make out part of the Antivirus software installed on each device, which in turn are monitored by a centralized virtual server.

The most evident form of attack on the Municipal network and systems are by means of spamming, which are filtered and monitored at server level already and further protected by the antivirus software installed on each device.

9.4.1.3.2.2 Security Software risk areas

With the approval of the PoPI act on 26 November 2013, various additional risks has been identified in terms of security software and what it should strive to prevent.

This act contains 8 principles, which make out the core of the act. These principles cover the following aspects:

1) Principle 1 – Accountability
2) Principle 2 – Processing Limitation (consent, justification etc.)
3) Principle 3 – Purpose Specification (purpose of collection, retention)
4) Principle 4 – Processing Limitation
5) Principle 5 – Information Quality (integrity of info)
6) Principle 6 – Openness (regulator notification)
7) Principle 7 – Security Safeguards
8) Principle 8 – Data Subject Participation (correction of info)

Although all of the principles are of the utmost importance principle 7 – Security Safeguards address the issue regarding security software directly.

Security Safeguards within **Principle 7** is an area where technology can assist the Municipality with the security challenge, while mapping to the PoPI framework & requirements.

The Act states the responsible party must take appropriate *reasonable* technical and organizational measures to prevent loss, unlawful access or damage to the information.

The Municipality needs to identify all reasonable potential risks, establish safeguards against these, and regularly verify these are effectively implemented. All these technical mechanisms need to be updated & reviewed frequently in response to the changing threat landscape.

Technologies and processes to address these are:

- Compliance suites
- Data Loss Prevention
- Encryption of Hard Drives and USB Drives
- Server System Protection
- Endpoint Protection
- Mobile Device Management
- Security Awareness Training

Questions to ask ourselves

1) How reliable is your current backup solution?
2) Is the current backup solution industry standard?
3) Is there accurate reporting on backup and deletion of data?
4) Is the backup solution standardized across the organization with central reporting?
5) Do you know what 'PoPI data' is leaving your organization?
6) Do you know where the sensitive data resides?
7) Can you confirm who has access to 'PoPI data'?
8) Is the infrastructure hosting 'PoPI data' secure and locked down?
9) How often are you doing updated vulnerability scans against your critical assets?
10) What is your encryption strategy regarding sensitive data?

11) Are your employee's aware of the basic security measures used to protect data?

12) How are you securing data on mobile devices & platforms?

13) How are you monitoring your internet facing devices and correlating this information?

The Municipality has addressed most of these above mentioned questions but there are still a lot of question to be answered in terms of these.

9.4.1.3.3 Access Control and CCTV

Who, What, Where and Why?

This should be the key question asked when considering the physical access and monitoring of all Municipal buildings and sites.

Looking at these question one should also take the financial viability of requirements and the integration to existing systems into consideration, while still having a keen sense of the business needs of the Municipality.

9.4.1.3.4 Current controls

The Municipality currently use an access control system, which mainly focus on the main building at Bredasdorp Head Office. This is the only current means of monitoring who has access to the Head Office, which is secured by using biometric access to the various locations in the affected buildings.

Although therefore we can assume that some sort of control measures are in place, we should not comfort ourselves in the thought that adequate security measures are in place and should strive towards better controlling access to our environment for means of access, data integrity, employee security and theft prevention of our assets.

9.4.1.3.5 Ensuring adequate security controls

Fundamentally the ideal will be to have a uniformed access control system, monitoring all building and sites of the Municipality while gaining additional functionality such as a time and attendance register and any other business need that should be deemed necessary.

Stakeholders in the Municipal environment will be a big part in the adaptation of such a system as it may have various functional and legislative requirements above the need for such security measures as deemed necessary by the ICT Department.

Key factors that may be taken into consideration are such as:

- Server room access
- Building or site access

- Sever room and or site monitoring by means of CCTV cameras
- HR modules implemented by CAM
- Time and attendance register
- Reporting capabilities
- Vehicle Tracking and vehicle users

9.4.1.3.6 Data Security

Data security being one of the most important security measures to be put in place are discussed here as the last point under the Security Framework, not because it is not important, but because if all the previous standards are met as set out in this framework mythology, it should be protected in its utmost form.

Scope of Work (SOW) related to ICT initiatives

- Implement CCTV with Analytics
- Enhance System and Network Security
- Upgrade / roll out Access Control

Benefits related to ICT initiatives

- Secure working environment
- Safer communities
- Data Integrity
- Safer Municipal Information Systems (MIS)
- Legislative compliance
- Improved information security and business continuity management

Risks related to ICT initiatives

- Security breaches
- Loss of Personal Information
- Reputational Risk
- Financial loss due to overtime spent
- Loss of key dependencies
- Loss of knowledge
- Legal penalties
- Inability to provide services
- Client dissatisfaction

Note: Risks will be managed in accordance to the risk management policy of the municipality around ICT.

Through the above items, points and/or considerations as context; the ICT initiative below has been identified:

1.	Implement CCTV with analytics set as a driver towards creating an enabling environment for economic growth and development and to create and maintain a safe and healthy environment												IDP Reference				SO. 4 SO. 12		
Year 1 (2017-2018)				**Year 2 (2018-2019)**				**Year 3 (2019-2020)**				**Year 4 (2020-2021)**				**Year 5 (2021-2022)**			
Q1	Q2	Q3	Q4	Q1	Q2	**Q3**	**Q4**	**Q1**	**Q2**	Q3	Q4	Q1	Q2	Q3	**Q4**	Q1	Q2	Q3	Q4
Champion(s):	Chief Information Officer / Protection Services																		
Department:	Finance & IT				**Completion by:**				2021/06				**Priority:**				L	M	**H**
Associated Costs:	Q1: R 0.00		C	O	Q2: R 1200 000		**C**	O	Q3: R 0.00		**C**	O	Q4: R 1000 000		**C**	O			
Total Project Value:	R 2300 000				**Total CAPEX:**		R 2 00 000				**Total OPEX:**		R 300 000						
Budget (Funded):	R 0 .00				**Unfunded:**		R 2 300 000				**Short:**		R 2 300 000						

Table 13: Objectives, Initiative and Business Case.

2.	Enhance system and network security set as a driver towards creating a culture of good governance and to create a culture of public participation and empower communities to participate in the affairs of the Municipality												IDP Reference				SO. 1 SO. 2		
Year 1 (2017-2018)				**Year 2 (2018-2019)**				**Year 3 (2019-2020)**				**Year 4 (2020-2021)**				**Year 5 (2021-2022)**			
Q1	Q2	Q3	Q4	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Senior ICT Specialist																		
Department:	Finance				**Completion by:**				2019/Q4				**Priority:**				L	M	**H**
Associated Costs:	Q1: R 62 500		C	**O**	Q2: R 62 500		C	**O**	Q3: R 62 500		C	**O**	Q4: R 62 500		C	**O**			
Total Project Value:	R 500 000				**Total CAPEX:**		R 0.00				**Total OPEX:**		R 500 000						
Budget (Funded):	R 100 000				**Unfunded:**		R 400 000				**Short:**		R 400 000						

Table 14: Objectives, Initiative and Business Case.

3.	Upgrade / roll out Access Control set as a driver towards creating a culture of good governance												IDP Reference				SO. 1		
Year 1 (2017-2018)				**Year 2 (2018-2019)**				**Year 3 (2019-2020)**				**Year 4 (2020-2021)**				**Year 5 (2021-2022)**			
Q1	Q2	**Q3**	Q4	Q1	Q2	**Q3**	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Senior ICT Technician																		

Department:	Finance			**Completion by:**			2018/Q3			**Priority:**			L	**M**	H
Associated Costs:	Q1: R 0.0	C	O	Q2: R 0.00	C	O	Q3: 300 000	**C**	O	Q4: R 0.00			C	O	
Total Project Value:	R 300 000			**Total CAPEX:**	R 300 000			**Total OPEX:**		R 0.00					
Budget (Funded):	R 300 000			**Unfunded:**	R 0.00			**Short:**		R 0. 00					

Table 15: Objectives, Initiative and Business Case.

9.4.1.4 Business Case 4: Business Continuity

Based on ISO/IEC 27031, ICT Readiness for Business Continuity (IRBC) [a general term for the processes described in the standard] supports Business Continuity Management (BCM) "by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization."

ICT readiness is important for business continuity purposes because:

- ICT is prevalent and many organizations are highly dependent on ICT supporting critical business processes;
- ICT also supports incident, business continuity, disaster and emergency response, and related management processes;
- Business continuity planning is incomplete without adequately considering and protecting ICT availability and continuity.

ICT readiness encompasses:

- Preparing organization's ICT (i.e. the ICT infrastructure, operation and applications), plus the associated processes and people, against unforeseeable events that could change the risk environment and impact ICT and business continuity;
- Leveraging and streamlining resources among business continuity, disaster recovery, emergency response and ICT security incident response and management activities.

ICT readiness should of course reduce the impact (meaning the extent, duration and/or consequences) of information security incidents on the organization.

The key focus areas relating to the ICT Business Continuity should include two aspects; Backup and Disaster Recovery and ICT Business Continuity plan.

9.4.1.4.1 Backup and Disaster Recovery

Data backup and disaster recovery are not the same. For one thing, the backup software can fail, or the person responsible for backing up can fail. In addition, backing up without recovery in mind is tantamount to not backing up at all. Finally, there are other steps you have to take in order to successfully restore your data in the event you need your backup. Steps like assembling the right recovery environment (the right operating

systems and servers and storage) and the right people, processes, and tools to bring back that backed up data.

A formally approved Disaster Recovery policy (DRF Policy) has been approved by Council in 2014, but the lacking of a formal policy of how backups should occur must enjoy immediate attention. This do not mean that no backup process are in place, hence the DR policy, but the formal documentation of the process and policy thereof must be drafted.

9.4.1.4.2 ICT Business Continuity Plan

Based on ISO/IEC 27031, the importance of a formal ICT Business Continuity plan are key to the success of the Municipality should a Disaster of any form occur, rendering the organization to such a state that business as usual cannot continue.

The drafting of such a plan will ensure that the Municipality can render business as either it has done in the current state or in such a way that fundamental services can continue without affecting the reputation of the Municipality.

This has to be done with keeping the Security Framework and Governance Framework of the Municipality in mind and still stay within the bounds of legislative requirements, such as the MFMA which include SCM procedures and policies

Scope of Work (SOW) related to ICT initiatives

- Upgrade ICT Disaster Recovery capabilities
- Implement ICT Disaster Recovery plan

Benefits related to ICT initiatives

- Disaster Management
- Reduce risk of Financial loss
- Enable the recovery of critical systems within an agreed timeframe
- Meet legal and statutory obligations
- Minimise the effect of a disruption on an organisation

Risks related to ICT initiatives

- Loss of Services
- Non Compliance
- Reduced productivity
- Municipal Information Systems not available
- Lack of Services Delivery

Note: Risks will be managed in accordance to the risk management policy of the municipality around ICT.

Through the above items, points and/or considerations as context; the ICT initiative below has been identified:

1.	Upgrade ICT Disaster Recovery capabilities set as a driver towards all Strategic objectives of the Municipality							IDP Reference			SO. 1 - 12								
Year 1 (2017-2018)				**Year 2 (2018-2019)**				**Year 3 (2019-2020)**				**Year 4 (2020-2021)**				**Year 5 (2021-2022)**			
Q1	Q2	Q3	**Q4**	**Q1**	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Senior ICT Specialist																		
Department:	Finance						**Completion by:**	2018/Q1			**Priority:**			L	M	**H**			
Associated Costs:	Q1: R500 000	C	O	Q2: R 0.00	C	O	Q3: R 0.00	C	O	Q4: R 0.00	**C**	O							
Total Project Value:	R 500 000			**Total CAPEX:**	R 500 000			**Total OPEX:**	R 0.00										
Budget (Funded):	R 500 00			**Unfunded:**	R 0.00			**Short:**	R 0.00										

Table 16: Objectives, Initiative and Business Case.

2.	Implement Disaster recovery plan set as a driver towards all Strategic objectives of the Municipality							IDP Reference			SO. 1 - 12								
Year 1 (2017-2018)				**Year 2 (2018-2019)**				**Year 3 (2019-2020)**				**Year 4 (2020-2021)**				**Year 5 (2021-2022)**			
Q1	Q2	Q3	Q4	Q1	Q2	**Q3**	**Q4**	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Champion(s):	Chief Information Officer																		
Department:	Finance						**Completion by:**	2018/Q4			**Priority:**			L	M	**H**			
Associated Costs:	Q1: R0.00	C	O	Q2: R 0.00	C	O	Q3: R 0.00	C	O	Q4: R 40 000	C	**O**							
Total Project Value:	R 50 000			**Total CAPEX:**	R 0.00			**Total OPEX:**	R 50 000										
Budget (Funded):	R 50 000			**Unfunded:**	R 0.00			**Short:**	R 0.00										

Table 17: Objectives, Initiative and Business Case.

9.4.2 Resource and Capacity Planning/Management

All the identified and defined initiatives will be governed by **ITIL** through usage of its **RACI** model/matrix which covers four (4) components, being; (a) Responsible, (b) Accountable, Consulted (c) and (d) Informed.

The RACI model is essentially geared towards providing or developing a single-view typology which speaks to everyone within the lifecycle, through a clearly defined understanding of all parties involved via various stages of the initiative(s) as described below:

1. Someone **Responsible** does the work.
2. Someone **Accountable** makes sure the work is done and signed-off.
3. Someone **Consulted** feeds back information into the process.
4. Someone **Informed** has information about the process broadcast to them.

For the purpose of simplicity and ease of understanding or use, the chart below provides context of **RACI** being utilised in its most basic form and aligned to the identified ICT initiative.

Initiative 1	End user computer refresh as part of Business case : ICT Infrastructure – Strengthening				
RACI	ICT Steering Committee	Senior Management	Chief Information Officer	Senior ICT Technician	ICT Technician
Provide device quantity requirements	I	R/C	I	A	I
Draft specifications	I		A/C	R	C
SCM processes handling	I		A	R	I
Roll out – setup and configuration of devices		I	A/C	R/C	R

Table 18: RACI model/matrix

A more in-depth output may however be achieved as below of when **RACI** is expansively mapped to an ICT initiative in holistic form.

Initiative 1	**End user computer refresh as part of Business case : ICT Infrastructure – Strengthening** Infrastructure									
RACI Matrix	**Project Leadership**		**Project Team Members**		**Project Sub-Teams**				**External Resources**	
Role / Deliverable (or Activity)	ICT Steering Committee	Chief Information Officer	Senior ICT Technician	ICT Technician	SCM Manager	BSC	BEC	BAC	Service Providers	Senior Management
Initiate Phase Activities										
- Request quantity requirements	I	I	A	A/R						C
- Submite quantity requirements	I	I	A/C	I/C						R/C
Plan Phase Activities										
- Research Solution / Specifications	I	A/C	R	C						
- Draft Specifications	I	A/C	R	C	C	C/A				
Execute Phase Activities										
- Submit SCM documentation	I	A/C	A/R	C	C					
- Review SCM documentation		A	A/R	I	C					
- Approval for procurement	I	C	I		C	A	A	A	I	
- Procure deliverables	I	A	R	I	C			I	R	
- Execute deliverables	I	I	A/R	R/C					I	I
Control Phase Activities										
- Perform Change Management	I	A/C	R	I/C						

Close Phase Activities	I	A	R	C						I

Table19: Expansive– RACI model/matrix.

Initiative 2	Implement public WI-FI services as part of Business case : ICT Infrastructure – Strengthening				
RACI	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technician	Service Provider
Provide achievable goals	A/C	I	A/R	I	C/I
Provide Business Case	I	C	A/R	C	C
Draft specifications	I	I	A/C	R	
SCM processes handling	I	I/C	A/R	R	
Implementation and control	I	I	A/R/C	R/C	R

Table 20: RACI model/matrix

Initiative 2	**Implement public WI-FI services as part of Business case : ICT Infrastructure – Strengthening**									
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**				**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	SCM Manager	BSC	BEC	BAC	Service Providers
Initiate Phase Activities										
- Meet with Council to determine their expectations	C	I	A/R	I						
- Draft Business Case for project	I	C	A/R	R	C					C
Plan Phase Activities										
- Research Solution / Specifications		I	A	R	C	C				
- Draft Specifications		I	A/R	R	C	I				
Execute Phase Activities										
- Submit SCM documentation		I	A	R	I	C				
- Review SCM documentation		I	C	R		A				

- Approval for procurement		I	C	R	I	C	A	A	A	I
- Procure deliverables	I	I	A	R	I	I				C
- Execute deliverables	I	I	A/R	C	C					R
Control Phase Activities										
- Perform Change Management		I	A	R	C					
Close Phase Activities	I	I	A	R	C					I

Table21: Expansive– RACI model/matrix.

Initiative 3	Develop Public Engagement Application as part of Business case : ICT Governance				
RACI	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technician	Service Provider
Provide achievable goals	A/C	I	A/R	I	C/I
Provide Business Case	I	C	A/R	C	C
Draft specifications	I	I	A/C	R	
SCM processes handling	I	I/C	A/R	R	
Implementation and control	I	I	A/R/C	R/C	R

Table 22: RACI model/matrix

Initiative 3	Develop Public Engagement Application as part of Business case : ICT Governance									
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**				**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	SCM Manager	BSC	BEC	BAC	Service Providers
Initiate Phase Activities										
- Meet with Council to determine their expectations	C	I	A/R	I						
- Draft Business Case for project	I	C	A/R	R	C					C
Plan Phase Activities										

- Research Solution / Specifications		I	A	R	C	C				
- Draft Specifications		I	A/R	R	C	I				
Execute Phase Activities										
- Submit SCM documentation		I	A	R	I	C				
- Review SCM documentation		I	C	R		A				
- Approval for procurement		I	C	R	I	C	A	A	A	I
- Procure deliverables	I	I	A	R	I	I				C
- Execute deliverables	I	I	A/R	C	C					R
Control Phase Activities										
- Perform Change Management		I	A	R	C					
Close Phase Activities	I	I	A	R	C					I

Table23: Expansive– RACI model/matrix.

Initiative 4	Implement CCTV with analytics as part of Business case: Security Framework				
RACI	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technician	Service Provider
Provide achievable goals	A/C	I	A/R	I	C/I
Provide Business Case	I	C	A/R	C	C
Draft specifications	I	I	A/C	R	
SCM processes handling	I	I/C	A/R	R	
Implementation and control	I	I	A/R/C	R/C	R

Table 24: RACI model/matrix

Initiative 4	Implement CCTV with analytics as part of Business case: Security Framework									
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**				**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	SCM Manager	BSC	BEC	BAC	Service Providers
Initiate Phase Activities										
- Meet with Council to determine their expectations	C	I	A/R	I						
- Draft Business Case for project	I	C	A/R	R	C					C
Plan Phase Activities										
- Research Solution / Specifications		I	A	R	C	C				
- Draft Specifications		I	A/R	R	C	I				
Execute Phase Activities										
- Submit SCM documentation		I	A	R	I	C				
- Review SCM documentation		I	C	R		A				
- Approval for procurement		I	C	R	I	C	A	A	A	I
- Procure deliverables	I	I	A	R	I	I				C
- Execute deliverables	I	I	A/R	C	C					R
Control Phase Activities										
- Perform Change Management		I	A	R	C					
Close Phase Activities	I	I	A	R	C					I

Table25: Expansive– RACI model/matrix.

Initiative 5	Enhance system and network security as part of Business case: Security Framework				
RACI	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technician	Service Provider
ICT Security Audit	I	I	A	C	R
Develop Business Case		I	A/R	C	C
Implementation plan	I	C	A	C	R
Solution implementation		I	A/C	C	R
Testing solution outcomes	I	I	A/R	C	R/C
Documentation and training		I	A	C	R

Table 26: RACI model/matrix

Initiative 5	**Enhance system and network security as part of Business case: Security Framework**								
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**		**External Resources**	
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	System Administrators	System Vendors	ICT Consultant / Support	Service Providers
Initiate Phase Activities									
- ICT Security Audit	I	I	A	C	C	I	I	R	
- ICT Security Audit report evaluation	I	R	A			I	C	C	
- Develop Business case		I	A/R	C	C	C	C	C	
Plan Phase Activities									
- Action / implementation plan	I	I	A	C	I	C	C	R	
- Create Schedule	I	I	A/R	C	I	C	I	C	
- Create Additional Plans as required	I	I	A/R	R	C	C	C	C	
Execute Phase Activities									
- Build deliverables			A	C	I			R	
- Procure deliverables	I	I	A/R	R	C			C	I
- Create status report			A/R	C		I		C	

Control Phase Activities									
- Perform Change Management		I	A	R	I	C	C	R	
Close Phase Activities									
- Create lessons learned	I	I	A/R	R	I	C	C	C	
- Closure and reporting	I	I	A/R	C	I	C	C	R	

Table27: Expansive– RACI model/matrix.

Initiative 6	Establish a fully functional Desktop Support Services as part of Business case : ICT Governance				
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	Human Resources	Service Provider
Appoint Helpdesk Official	C	A	I	R	
Research solution	I	A	R		C
Solution implementation	I	A	R		R/C
Testing solution outcomes	I	A/I	R		C
Documentation and training	I	A/C	R		R

Table 28: RACI model/matrix

Initiative 6	**Establish a fully functional Desktop Support Services as part of Business case : ICT Governance**							
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**		**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	System Administrators	System Vendors	ICT Consultant / Support
Initiate Phase Activities								
- Submit Project Request	R	I	A	C		C		
- Develop Job description		I	A/R	C		C		

- Develop Business case	I	I	A/R	C	C	C		C
Plan Phase Activities								
- Create Schedule		I	A/R	C		C	C	
- Action / implementation plan			A	C		R	I	
- Create Additional Plans as required			A	I		R	C	I
Execute Phase Activities								
- Build deliverables			C	C	I	A/R	C	C
- Create status report		I	A			R	C	
Control Phase Activities								
- Perform Change Management		I	A	C		R		
Close Phase Activities								
- Create lessons learned and SOP`s			A	C		R	I	C
- Closure and reporting		I	A	C		R		

Table29: Expansive– RACI model/matrix.

Initiative 7	Upgrade / roll out Access Control as part of Business case: Security Framework				
RACI	ICT Steering Committee	Senior Management	Chief Information Officer	Senior ICT Technicians	ICT Technician
Provide site requirements	I	R/C	I	A	I
Draft specifications	I		A/C	R	C
Roll out – setup and configuration of devices		I	A/C	R/C	R
Reporting	I	I	A	R	C

Table 30: RACI model/matrix

Initiative 7	Upgrade / roll out Access Control as part of Business case: Security Framework							
RACI Matrix	Project Leadership			Project Team Members		Project Sub-Teams		External Resources
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	System Administrators	System Vendors	ICT Consultant / Support
Initiate Phase Activities								
- Submit Project Request	R	I	A	C		C		
- Research solution		I	A	C		R	C	C
- Develop Business case	I	I	A	C	C	R	C	C
Plan Phase Activities								
- Create Schedule		I	A	C		R	C	
- Action / implementation plan			I	C		A	R	
- Create Additional Plans as required			A	I		R	C	I
Execute Phase Activities								
- Build deliverables			C	C	I	A	R	C
- Create status report		I	A			R	C	
Control Phase Activities								
- Perform Change Management		I	A	C		R	C	C
Close Phase Activities								
- Create lessons learned and SOP`s			A	C		R	I	C
- Closure and reporting		I	A	C		R		

Table 31: Expansive– RACI model/matrix.

Initiative 8	Implement Mail Archiving solutions as part of Business case: ICT			
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	Service Provider
Research solution	I	A	R	C
Solution implementation	I	A	R	R/C
Testing solution outcomes	I	A/I	R	C

Documentation and training	I	A/C	R	R

Table 32: RACI model/matrix

Initiative 8	Implement Mail Archiving solutions as part of Business case: ICT Governance							
RACI Matrix	Project Leadership			Project Team Members		Project Sub-Teams		External Resources
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	System Administrators	System Vendors	ICT Consultant / Support
Initiate Phase Activities								
- Submit Project Request	R	I	A	C		C		
- Research solution		I	A	C		R		C
- Develop Business case	I	I	A/R	C	C	C		C
Plan Phase Activities								
- Create Schedule		I	A/R	C		C	C	
- Action / implementation plan			A	C		R	I	
- Create Additional Plans as required			A	I		R	C	I
Execute Phase Activities								
- Build deliverables			C	C	I	A/R	C	C
- Create status report		I	A			R	C	
Control Phase Activities								
- Perform Change Management		I	A	C		R		
Close Phase Activities								
- Create lessons learned and SOP`s			A	C		R	I	C
- Closure and reporting		I	A	C		R		

Table33: Expansive– RACI model/matrix.

Initiative 9	Upgrade ICT Disaster Recovery capabilities as part of Business case: Business Continuity			
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	Service Provider
Research solution	I	A	R	C
Solution implementation	I	A	R	R/C
Testing solution outcomes	I	A/I	R	C
Documentation and reporting	I	A/C	R	R

Table 34: RACI model/matrix

Initiative 9	**Upgrade ICT Disaster Recovery capabilities as part of Business case: Business Continuity**							
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**		**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	System Administrators	System Vendors	ICT Consultant / Support
Initiate Phase Activities								
- Submit Project Request	C	I	A/R	C		C		
- Research solution		I	A	R	I	C	I	C
- Develop Business case	I	I	A/R	C	C	C	I	C
Plan Phase Activities								
- Create Schedule		I	A/R	C		C	I	C
- Action / implementation plan			A	R		C	I	C
- Create Additional Plans as required			A	R		I	C	I
Execute Phase Activities								
- Build deliverables			C	A	I	I	R	C
- Create status report		I	A	R		I	C	
Control Phase Activities								
- Perform Change Management		I	A	R		C		
Close Phase Activities								

- Create lessons learned and SOP`s			A	R		C	I	C
- Closure and reporting		I	A	R		C		

Table35: Expansive– RACI model/matrix.

Initiative 10	Implement ICT Disaster recovery plan as part of Business case: Business Continuity						
RACI	Executive Council	ICT Steering Committee	Chief Information Officer	ICT DR Team	Senior ICT Technicians	ICT Technician	System Administrators
Assemble ICT DR Team	I	A/R	C	I			I
Research solutions		I	A/C	I	R	C	C
Implement Technologies		I	A	I	R	C	C
Testing Plan	I	A/R	R	R	C	C	R
Review Plan	I	I	A/R	C	C	I	C

Table 36: RACI model/matrix

Initiative 10	**Implement ICT Disaster recovery plan as part of Business case: Business Continuity**								
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**		**External Resources**	
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	ICT DR TEAM	System Administrators	System Vendors	ICT Consultant / Support
Initiate Phase Activities									
- Assemble ICT DR Team		A/R	C			I	I		
- Communicate Status, ICT DRP to line Mangers and Municipal Mgt.		A	R	I	I	I	C		
Plan Phase Activities									
- Facilitate Bus Impact & Risk Analysis with Line Managers		I	A/R	R	I	I	C	C	

- Requirements to be supplied to Head of ICT		A	I			R	C		C
Execute Phase Activities									
- Strategy: Review Recover Approach & Technology Architecture		I	A/R	R	C	I	C	C	C
- Define initiatives for Technology Upgrades, business case and cost to address gaps		C	A/R	R	C	I	C	C	C
- Implement Technology initiatives		I	A	R	C	I	R	C	C
Control Phase Activities									
- Address gaps in ICT DR Plan and Definition for Architecture documents and update		I	R	C	C	A	C	C	C
- Testing of ICT DR plan		I	R	R	I	A	C	C	I
Close Phase Activities									
- Identify gaps & assign tasks to improve ICT DR Plan		I	R	C	C	A	C	C	C
- Review, audit preparation		I	R	C	C	A	C	I	I

Table37: Expansive– RACI model/matrix.

Initiative 11	**Establish and implementing Intranet as part of Business case: ICT Governance**				
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	Communications Division	Service Provider
Research solution	I	A	R	C	C
Solution implementation	I	A	R	I	R/C
Testing solution outcomes	I	A	R	R	C
Documentation and training	I	A/C	R	C	R

Table 38: RACI model/matrix

Initiative 11	Establish and implementing Intranet as part of Business case: ICT Governance							
RACI Matrix	Project Leadership			Project Team Members		Project Sub-Teams		External Resources
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	Communications Division	System Administrators	System Vendors	ICT Consultant / Support
Initiate Phase Activities								
- Submit Project Request	R	I	A	C	C	C		
- Research solution		I	A	C	C	R		C
- Develop Business case	I	I	A/R	C	C	C		C
Plan Phase Activities								
- Create Schedule		I	A/R	C	C	C	C	
- Action / implementation plan			A	C	I	R	I	
- Create Additional Plans as required			A	I	C	R	C	I
Execute Phase Activities								
- Build deliverables			C	C	I	A/R	C	C
- Create status report		I	A		I	R	C	
Control Phase Activities								
- Perform Change Management		I	A	C		R		
Close Phase Activities								
- Create lessons learned and SOP`s			A	C	C	R	I	C
- Closure and reporting		I	A	C	I	R		

Table39: Expansive– RACI model/matrix.

Initiative 12	**Upgrading of Wide Area Network as part of Business case: ICT Infrastructure – Strengthening ICT Infrastructure**			
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	Service Provider
Research solution	I	A	R	C
Solution implementation	I	A	R	R/C

Testing solution outcomes	I	A/I	R	C
Documentation and reporting	I	A/C	R	R

Table 40: RACI model/matrix

Initiative 12	**Upgrading of Wide Area Network as part of Business case: ICT Infrastructure – Strengthening ICT Infrastructure**							
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**		**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	Remote Users	System Vendors	ICT Consultant / Support
Initiate Phase Activities								
- Submit Project Request	I	I	A/R	C				
- Research solution			A	R	I		C	C
- Develop Business case		I	A/R	C	C	I	C	C
Plan Phase Activities								
- Create Schedule		I	A/R	C			C	I
- Action / implementation plan			A	R	I	I	C	C
- Create Additional Plans as required			A	R	I			C
Execute Phase Activities								
- Build deliverables			C	A	I		R	C
- Create status report		I	I	A		C	R	I
Control Phase Activities								
- Perform Change Management		I	A	R		C		
Close Phase Activities								
- Create lessons learned and SOP`s			A	R		C	C	I
- Closure and reporting		I	A	R		C	I	I

Table41: Expansive– RACI model/matrix.

Initiative 13	Upgrading of Local Area Network as part of Business case: ICT Infrastructure – Strengthening ICT Infrastructure			
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technician	Product Vendors
ICT Network Audit	I	A	R	
Develop Business Case	I	A/R	C	
Implementation plan	C	A	R	C
Solution implementation	I	A/C	R	C
Testing solution outcomes	I	A	R	C
Documentation and training	I	A/C	R	

Table 42: RACI model/matrix

Initiative 13	**Upgrading of Local Area Network as part of Business case: ICT Infrastructure – Strengthening ICT Infrastructure**							
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**		**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	System Administrators	Vendors	ICT Consultant / Support
Initiate Phase Activities								
- ICT Network Audit	I	I	A	R	C	I		C
- ICT Network Audit report evaluation	I	R	A			I		C
- Develop Business case		I	A/R	C	C	C		C
Plan Phase Activities								
- Action / implementation plan	I	I	A	R	I	C		C
- Create Schedule	I	I	A/R	C	I	C		C
- Create Additional Plans as required	I	I	A/R	R	C	C		C
Execute Phase Activities								
- Build deliverables			A	R	I			C

- Procure deliverables	I	I	A/R	R	C		I	I
- Create status report			A/R	C		I		C
Control Phase Activities								
- Perform Change Management		I	A	R	I	C		
Close Phase Activities								
- Create lessons learned	I	I	A	R	I	C		C
- Closure and reporting	I	I	A/R	C	I	I		C

Table43: Expansive– RACI model/matrix.

Initiative 14	**Upgrading Internet Connectivity as part of Business case: ICT Infrastructure – Strengthening ICT Infrastructure**			
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	Service Provider
Research solution	I	A	R	C
Solution implementation	I	A	R	R/C
Testing solution outcomes	I	A/I	R	C
Documentation and reporting	I	A/C	R	R

Table 44: RACI model/matrix

Initiative 14	**Upgrading Internet Connectivity as part of Business case: ICT Infrastructure – Strengthening ICT Infrastructure**							
RACI Matrix	**Project Leadership**			**Project Team Members**		**Project Sub-Teams**		**External Resources**
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	Remote Users	System Vendors	ICT Consultant / Support
Initiate Phase Activities								
- Submit Project Request	I	I	A/R	C				
- Research solution			A	R	I		C	C
- Develop Business case		I	A/R	C	C	I	C	C

Plan Phase Activities								
- Create Schedule		I	A/R	C			C	I
- Action / implementation plan			A	R	I	I	C	C
- Create Additional Plans as required			A	R	I			C
Execute Phase Activities								
- Build deliverables			C	A	I		R	C
- Create status report		I	I	A		C	R	I
Control Phase Activities								
- Perform Change Management		I	A	R		C		
Close Phase Activities								
- Create lessons learned and SOP`s			A	R		C	C	I
- Closure and reporting		I	A	R		C	I	I

Table45: Expansive– RACI model/matrix.

Initiative 15	**Develop an ICT Maintenance plan as part of Business case: ICT Governance**			
RACI	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Service Provider / Support
ICT Site file Audit	I	A/C	R	C
Develop Business Case	I	A/R	C	C
Research best practices	I	A	R	C
Solution implementation	I	A	R	C
Testing solution outcomes	A	R	C	I
Documentation and approval	A	R	C	I

Table 46: RACI model/matrix

Initiative 15	Develop an ICT Maintenance plan as part of Business case: ICT Governance							
RACI Matrix	Project Leadership			Project Team Members		Project Sub-Teams		External Resources
Role / Deliverable (or Activity)	Executive Council	ICT Steering Committee	Chief Information Officer	Senior ICT Technicians	ICT Technician	System Administrators	Vendors	ICT Consultant / Support
Initiate Phase Activities								
- ICT Site file Audit		I	A	R	C	C	C	C
- ICT Site file Audit report evaluation		A/R	C	I		I		
- Develop Business case		I	A/R	R	C	C	C	C
Plan Phase Activities								
- Action / implementation plan		I	A/R	R	C	C		
- Create Schedule		I	A/R	C	I	I	I	C
- Create Additional Plans as required		I	A	R	I	I	I	C
Execute Phase Activities								
- Research best practices			A	R	C	C	C	C
- Draft Maintenance plan			A/R	C	I	C	C	C
- Create status report		I	A/R	C				
Control Phase Activities								
- Table draft plan		I	A/R	C				
- Adopt plan as policy of Municipality	A/R	I	C			I		
Close Phase Activities								
- Create lessons learned	I	I	A	R		C	C	I
- Closure and reporting	I	I	A	R		C		I

Table47: Expansive– RACI model/matrix.

10 ICT Status Quo

This section is specifically to provide an overview around the current ICT landscape of the municipality, while simultaneously providing context towards the guidance on strategic direction of this document. A *Book of Standards* has been identified and developed for the municipality towards consideration of the ICT portfolio. This *Book of Standards* defines the standards in place within the municipality around their ICT environment i.e.

including but not limited to; standards around End User Machine types/specs, standards around Storage systems/platforms, standards around Networking equipment/infrastructure, etc., then will be added as *Addendum 6* accompanying this document. Additional items may be filled in as required by the municipality.

10.1 Current ICT Portfolio

This document is to ensure that all items related to a holistic strategy and the according implementation plan(s) be considered through having not only understanding around IDP or ICT objectives and initiatives, but rather so also having expansive insight into the current (existing) ICT portfolio and environment.

The ICT portfolio stack consists (but are not limited to) of the following categories, with the municipality providing sufficient detail as a high-level overview to each of the categories, including particulars around the infrastructure/equipment. The ICT portfolio stack is viewed from a high-level perspective, but may be expanded upon as required. The stack consists, but not are not limited to the following sections:

1. Networking, which may further be unpacked under WAN, LAN, SDN, IAAS and PAAS.
2. Wireless, which may further be unpacked under WAN and/or LAN.
3. Servers, which may further be unpacked under VM's, HV's, Hosted/Cloud and Physical.
4. Security, which may be further unpacked under WAN, LAN, Core and End User.
5. Storage, which may further be unpacked under VM's, HV's, Hosted/Cloud, Physical.
6. Operating Systems, which may further be unpacked as required.
7. End User Workstations, which may further be unpacked as required.
8. Telephony, which may further be unpacked under PABX, PBX, IP, SIP, IAAS, PAAS, Hosted/Cloud and Physical.
9. Peripherals, which may further be unpacked under Print, Scan and Docking Stations.
10. Video Conferencing, which may further be unpacked under Physical, Hosted/Cloud, IAAS and PAAS.
11. Cloud or Hosted, which may further be unpacked under IAAS, PAAS and SAAS.
12. Disaster Management/Recovery, which may further be unpacked under VM, VA, Hosted/Cloud, and Physical.
13. Service Providers with SLA's

Each category will be broken down into its own sub-section for ease of identification and understanding of the various items comprising of the specific category i.e.; Servers may be unpacked into Physical and Virtual, etc.

10.1.1 Networking

Networking being the backbone, ensuring adequate efficient and effective service delivery when utilizing systems and devices, is fundamental to not only control the environment utilizing these systems and devices but also ensuring a secure safe environment.

By focusing on a standardized approach in networking and networking devices, the Municipality can ensure that the environment is as accessible and secure as possible, to those who has rights to these networks.

Networks consist of both physical and wireless infrastructure in so connecting the various users, which in turn rely on both the ICT division and external service providers to manage the environment.

By focusing on HP switches on the local area network and standardizing to this, we can ensure that relevant PoE devices and security protocols such as radius servers, utilizing the 802.1x protocols, can be implemented encompassing a Sophos firewall and related products.

Provisioned with the utilization of HP Switches is the lifetime warrantee that holds a huge cost benefit to the Municipality, should these devices become faulty.

Wide area networks (WAN) are currently outsourced amongst other things due to the lack of skill and resources to manage such an environment. The rate at which these this type technology change can be immense and therefore, by outsourcing this service, the Municipality can transfer the risk relating to the upkeep of such a network, as well as the replacement of these network devices to a 3rd party. The main focus should then be on Managing the service provider and the cost relating to these services.

10.1.2 Wireless

Access has to be as secure as possible and the management thereof is as important as the utilization thereof. With this in mind and security protocols as mentioned under the network section previously, the Municipality implemented integrated Sophos wireless infrastructure ensuring access to these networks are managed and controlled.

10.1.3 Servers

This refers to the hosting environments or platforms on which the various Municipal Information Systems (MIS) of the Municipality runs.

This can be defined as one of the most important infrastructure devices as information hosted on these servers are key to providing information and services to communities.

One has to consider the environment these servers are located in and also how to best ensure the availability thereof. Question has to be asked like; Where are these servers, what is on them and what will happen when they become faulty or redundant?

Taking these question into account one may consider that by Standardizing on Dell server as the Municipality did, can ensure that systems are compatible, running in the same environment and assist with ensuing failover or redundancy is in place.

Cost benefit relating to this is that when standardizing on these Dell Servers, fewer types of replacement parts has to be kept onsite, which may be required to minimize downtime. This is measured versus hosting Servers of different manufacturers that use different parts and does not necessarily ensure compatibility. Hence, extra resources has to be made available to address these issues.

10.1.4 Security

A holistic approach has fundamental in securing the ICT environment.

This approach ensure that both physical and electronic controls are in place, safeguarding the environment within which the Municipality functions.

The purpose is to provide edge-to-edge protection without compensating on accessibility to allowed stakeholders. In managing this environment, the Municipality may need to consider Governance structures, physical hardware, software and human factors.

As previously mentioned the Municipality protects its edge network utilizing a hardware firewall, it also utilize Sophos Antivirus software that acts as a software firewall at end user level. Furthermore, a radius server system has been implemented that still needs to be expand to all relevant sites.

Third Party management is as important, especially with the frequent request to access the network of the Municipality to provide various services. Processes and control managing this is fundamental in ensuring that not only the environment is safeguarded, but also to ensure we adhere to applicable legislation.

10.1.5 Storage

Reliance on systems are becoming more relevant on a daily basis. The downside to this is that the rate at which information is generated becomes reliant on additional storage space, as it may need to be accessed again at a later stage. Second to this, this information then has to be kept safe, secure and must be available on backup for a certain legislative prescriptive time.

On board storage and Network Attached Storage (NAS) devices is currently being utilized in the Municipality, but centralized shared storage for virtual environments may be deemed necessary in the future, dependent on the growth or users need for additional systems or storage. The probability of Cloud storage may also need to be investigated in the future, but this is still reliant on legislation and infrastructure availability, considering our geographical location as well.

10.1.6 Operating Systems

Operating system is the software that run on a device to ensure the device can perform its set function.

Microsoft is the main operating system currently utilized by the Municipality for both Servers and end user devices such as desktop and laptops. Although one can use other Operating systems such as IOS and Linux based system, one has to consider how these system will integrate and/or if these system are compatible with each other. One of the biggest drivers to, why Windows operating system, are the new mSCOA reform, being prescriptive on utilizing a Microsoft based database structure, SQL.

10.1.7 End User Workstations

Compatibility, availability and interchangeability is one of the key considerations when standardizing on end user workstations. These devices is tools utilize by Officials in the Municipality in order to assist with Service Delivery therein.

With a limited budget and support staff to ensure the functionality of these devices in the cases where they become faulty, one has to think of ways to reduce the downtime thereof. With this in mind and as in the case of servers, where one has to carry stock on parts for various type of devices, the Municipality has begun to standardize on Dell end user workstations, which include both desktop and laptops.

Due to the location of the Municipality, support and parts are not always available and procurement of parts can take a while due to various reasons. Because of this, through past experiences and lessons learned, it has been found that Dell provide the best next business onsite support in our area and in so limit the downtime of devices to the minimum.

10.1.8 Telephony

The telephone system are currently outsourced amongst other things due to the lack of skill and resources to manage such an environment. The rate at which these this type technology change can be immense and therefore, by outsourcing this service, the Municipality can transfer the risk relating to the upkeep of such a system, as well as the replacement of these systems and devices to a 3rd party. The main focus should then be on Managing the service provider and the cost relating to these services.

10.1.9 Peripheral (Print, Scan, Docking Stations, etc.)

After a comprehensive investigation, the Municipality has found it more cost effective in outsourcing these services.

One of the key rational behind this was due to the specialized skills required for repairing such devices, should they become faulty, the downtime thereof and the impact it may have on service delivery.

By managing this service by means of a SLA, one can minimize downtime, but also monitor cost relating to this service.

10.1.10 Video Conferencing

The purpose of this facility is to enable individuals inside and outside the Municipality to communicate visually with the same functionality they would have had if they`ve met in person. This include file sharing, whiteboards, presentations and recording capabilities.

This function has been readily available in the Municipality for internal use by historically utilizing the Microsoft Lync, now better known as Skype for business.

Various service providers currently utilize Skype for Business at their organizations as well and therefore in can be recommended that the Municipality investigate the possibility to implement an edge server to allow us to communicate with these organization seamlessly as well.

In addition to this the probability of using video conferencing as a shared services between Municipalities in the District can also be investigated, as it can lead to cost and time savings in terms of various divisions of the respective Municipalities being able to meet, without traveling to one another.

10.1.11 Cloud or Hosted

Cloud computing can be defined as the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer

The Municipality do not utilize cloud by means of Platform as a service (PaaS) defined as, a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

This means that most of our Information systems is hosted in-house in our own data center.

We do however utilize the cloud environment for some services such as Ignite our performance and complaints system, online viewing of Municipal accounts and the hosting of our website.

The probability of Cloud storage may also need to be investigated in the future, but this is still reliant on legislation and infrastructure availability, considering our geographical location as well.

10.1.12 Disaster Management/Recovery

This category is especially reliant on the infrastructure relating to the heading previously mentioned in this section. The hardware we use for the various functions is key to the success of Disaster Management /Recovery and the planning thereof.

Although the Municipality do have an identified Disaster Recovery site where daily backups are send via the WAN utilizing Quest Dell Rapid Recovery software, the implementation, testing and auditing of an adopted Disaster Recovery plan is key to the success of this functionality.

10.1.13 Service Providers with SLA's

The delivery of ICT services to the Municipality require specialist skills and varying capacity demands. The use of external service providers/vendors to provide ICT services can be a cost effective and reliable way of acquiring these skills at a reasonable cost and in the required timeframes. As a result, information security risks also extend across the supply chain and therefore service providers/vendors of ICT related services must be managed to ensure that these risks are controlled and mitigated where possible. ICT remains accountable for ICT services under the control of service providers/vendors. It is for this reason that the management of service providers/vendors is an important Municipal task to ensure that service providers/vendors deliver the agreed services within the agreed timeframes and cost.

10.2 Assessment(s)

Through the review of the ICT environment and its existing portfolio; assessments on the state of specific systems, services or solutions of ICT within the municipality towards consideration has been noted as:

With reviewing the aforementioned/listed portfolio stack, one can derive that although various implementations, systems or projects has been implemented, the ever-changing environment has to be considered as well.

One need to consider how influences both internal and external to the Municipality can affect these listed items and what the capacity of the Municipality is to address these changes. They key however should be on how these instances is and can be used as a driver towards meeting the goals of Council in delivering services to the community.

1. Security relating to the network is fundamental and measure has to be taken in order to safeguard the ICT environment whilst ensuring the infrastructures capabilities address the need as set out by the relevant stakeholders.
2. Wireless access and security may be as relevant to internal users and 3rd parties as in the case of the physical network, but expanding a wireless network or pubic Wi-Fi may also be considered, especially if it can add value to both the Municipality and the community.
3. Servers being the backbone for system is fundamental in delivering services and by ensuring Maintenance plan is in place the upkeep of these systems can be mitigated more efficiently rather than running into unforeseen problems.
4. Security of both the physical - and electronic environment is key to data integrity and plans should be put in place, addressing current shortfalls and possible future risks.
5. Storage is a manageable resource, but should it be left unattended can have a significant impact on the organization. Once again, with the utilization of well-developed maintenance plan and a good governance structure in place, planning of this resource can be dealt with in a controlled manner.
6. Video conferencing is becoming more relevant in the day and age we live in and the investigation of such a functional reliable system can hold many benefits to the Municipality. One just need to be aware of all the factors involved in such a services, inclusive of Internet availability, bandwidth and redundancy.

7. Cloud computing is becoming more applicable and can lead to cost savings and lesson the strain on operational management, in so addressing the issue of drain on resources. One just need to be vary of the various legislations applicable to such a solution, as data is one of the biggest assets of the Municipality.

10.3 Current ICT Costs

Spend associated to the existing operations of ICT is to be noted to establish insight into understanding and forecasting, with a driver being that this document shall serve as confirmation, motivation and authorization of budget towards ICT and its all-encompassing future or intended undertakings.

A single yet comprehensive table as noted below will embody all cost associations related to ICT within the municipality.

Note: The costs below to be identified are aligned to the Municipal Standard Charter Accounts (mSCOA).

Category	Details	Amount (2016 – 2017)
Human Capital Resources	**Total Cost/Spend for Category (Staffing)**	**R 1 887 661**
Total cost of employment for ICT related resources including contracting for projects and outsourced/managed services.	Permanent (Official)	R 1 437 661
	Contractual (Projects)	R 450 000
	- Outsourced Services (Agreements)	R 90 000
	- Consultant and Professional Services	R 360 000
	- Maintenance of equipment/assets	R 0
CAPEX	**Total Cost/Spend for Category (CAPEX)**	**R 1 370 900**
Hardware (All assets that depreciates over a period of time due to it being a physical medium/equipment.)	Networking	R 25 000
	Wireless	R 0
	Servers	R 198 000
	Computer / Laptops / Screens	R 220 900
	Backup devices / peripherals	R 59 000
	UPS	R 7000
	Generators	R 220 000
	Projectors	R 24 000
	Two way radios	R 59 000
Auxiliary Infrastructure (ICT items required as supplementary to enable official ICT items i.e. Hardware to function.)	Data Cabling	R 0
	Development	R 0
	Hosted and Cloud	R 0
	Safran T/A clocks. Controllers and peripherals	R 200 000
Software (Licenses and ad hoc	Corel Draw	R 8 000
	Kronos / Saflec	R 350 000
OPEX	**Total Cost/Spend for Category (OPEX)**	
Software (Licenses and ad hoc licenses/purchases.)	Microsoft	R 960 000
	Cloud/Hosted	R 12 000
	Third Party Applications	
	- Municipal Information systems	R 1 603 380
	- ICT related applications	R 430 000

Service Level Agreements	Microsoft Windows Server Support Services	R 0
	Managed Services Provider	R 575 600
Contracted services	Consultancy	R 100 000
Maintenance	Data Cabling	R 15 000
	Hosted and Cloud	R 12 000
	Computer peripherals	R 74 000
	Printers	R 30 000
General expenses	Conferences and seminars	R 1 500
	Consumables	R 500
	Printer consumables	-
	Printing & stationery	R 1 100
	Refreshments	R 1 000
	Subsistence and travelling officials	R 7 500
	Sundry expenses	R 1 000
	Telecommunications: cell phones	R 21 600
	Telecommunications: data lines	R 850 000
	Telecommunications: telemetric systems	R 80 000
	Telecommunications: telephone	R 2 500
	Travel exp: accommodation	R 17 900
	Travel exp: transportation	R 18 500

Table 48: Holistic Current ICT Costs/Spend.

11 Roadmap

The ICT roadmap is a key enabler to the ICT strategy, whereby it provides a holistic view across the entire lifecycle of this strategy. The aforementioned ICT initiatives are born through meeting of objectives, providing full context in detail of each specific initiative. Whereas the roadmap itself, instead seeks to provide context around all of the combined initiatives, for the duration of the lifecycle.

As taken from the ICT initiatives through the aforementioned '*Department's ICT Objectives'* section, we may note that there are officially [R 19 040 000] that have been identified. As a high-level view, they are noted as:

1. End User Computer Refresh
2. Implement Public Wi-Fi Service
3. Develop Public Engagement App.
4. Implement CCTV with analytics
5. Enhance system and network security
6. Establish a fully functional Desktop Support Services
7. Upgrade / roll out Access Control
8. Implement Mail Archiving solution
9. Upgrade ICT Disaster Recovery capabilities
10. Implement Disaster Recovery plan
11. Establishing and implementing Intranet
12. Upgrading of Wide Area Network (WAN)

13. Upgrading of Local area network (LAN)
14. Upgrade Internet Connectivity
15. Develop an ICT Maintenance plan.

11.1 Implementation Plans

As a complete unified view; the table below *(Table 49)* is noted as an example to ensure ease of understanding towards all ICT initiatives, including a key legend for tracking, specifically due to this document being reviewed on an annual basis and items are tracked throughout the entire lifecycle and versions of this document.

Note: The implementation plan is aligned to the migration plan as identified and prescribed in the MCGICTP.

Official 5 Year Implementation Plan: 2017 – 2022																				
	YEAR 1				YEAR 2				YEAR 3				YEAR 4				YEAR 5			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
End User Computer Refresh **IDP Reference # SO. 8**																				
Implement Public Wi-Fi Service **IDP Reference # SO. 2 - SO. 4 - SO. 5 - SO. 9 - SO. 11**																				
Develop Public Engagement App. **IDP Reference # SO. 2 - SO. 5 - SO. 9**																				
Implement CCTV with analytics **IDP Reference # SO. 4 - SO. 12**																				
Enhance system and network security **IDP Reference # SO. 1 - SO. 2**																				
Establish a fully functional Desktop Support Services **IDP Reference # SO. 1**																				
Upgrade / roll out Access Control **IDP Reference # SO. 1**																				
Implement Mail Archiving solution **IDP Reference # SO. 1 - SO. 3**																				
Upgrade ICT Disaster Recovery capabilities **IDP Reference # SO. 1 - 12**																				
Implement Disaster Recovery plan **IDP Reference # SO. 1 - 12**																				
Establishing and implementing Intranet **IDP Reference # SO. 3**																				
Upgrading of Wide Area Network (WAN) **IDP Reference # n/a**																				
Upgrading of Local area network (LAN) **IDP Reference # n/a**																				
Upgrade Internet Connectivity **IDP Reference # n/a**																				

Develop an ICT Maintenance plan. **IDP Reference # n/a**																			

Table 49: 5 Year Implementation Plan(s).

11.2 Alignment of National & Provincial Initiatives

In the IDP process of Council the National and Provincial Initiatives has been considered and in so the alignment of this strategic document to the Municipal approved IDP, aligned to the objectives thereof, ensure the alignment to the set National and Provincial goals.

11.3 Budget Breakdown/Structure

Within this section, we will review the holistic budget and set it into different sub-sections for ease of identification and understanding. This provides the municipality alongside its stakeholder's full perspective through adequate articulation of costs, some being noted as but not limited to, per-quarter costs for individual initiative or a collection of all initiatives, to the total yearly cost per initiative or for all initiatives combined.

11.3.1 Budget - Year 1

This section provides full view of the first year as the initiation year related to the five (5) year implementation plan(s).

Official 5 Year Implementation Plan Budget: YEAR 1					
Identified ICT Initiatives	2017 – 2018				
	Q1	Q2	Q3	Q4	TOTAL
End User Computer Refresh **IDP Reference # SO. 8**		300 000			300 000
Upgrade / roll out Access Control **IDP Reference # SO. 1**			200 000		200 000
Upgrade ICT Disaster Recovery capabilities **IDP Reference # SO. 1 - 12**				300 000	300 000
Upgrading of Local area network (LAN) **IDP Reference # n/a**		50 000			50 000
Upgrading of Wide Area Network (WAN) **IDP Reference # n/a**			150 000	150 000	300 000
Collective Totals:		**350 000**	**350 000**	**450 000**	**1 150 000**

Table 50: 5 Year Implementation Plan Budget, Year 1.

11.3.2 Budget - Year 2

This section provides full view of the second year as the midway point related to the five (5) year implementation plan(s).

Official 5 Year Implementation Plan Budget: YEAR 2					
Identified ICT Initiatives	2018 – 2019				
	Q1	Q2	Q3	Q4	TOTAL
End User Computer Refresh **IDP Reference # SO. 8**		300 000			300 000
Implement CCTV with analytics **IDP Reference # SO. 4 - SO. 12**			100 000	200 000	300 000
Enhance system and network security **IDP Reference # SO. 1 - SO. 2**	62 500	62 500	62 500	62 500	250 000
Establish a fully functional Desktop Support Services **IDP Reference # SO. 1**	72 500	72 500	72 500	72 500	290 000
Upgrade / roll out Access Control **IDP Reference # SO. 1**			100 000		100 000
Implement Mail Archiving solution **IDP Reference # SO. 1 - SO. 3**		250 000			250 000

Upgrade ICT Disaster Recovery capabilities **IDP Reference # SO. 1 - 12**	200 000				200 000
Implement Disaster Recovery plan **IDP Reference # SO. 1 - 12**				50 000	50 000
Establishing and implementing Intranet **IDP Reference # SO. 3**				50 000	50 000
Upgrading of Wide Area Network (WAN) **IDP Reference # n/a**	150 000	150 000	150 000	150 000	600 000
Upgrading of Local area network (LAN) **IDP Reference # n/a**		50 000			50 000
Upgrade Internet Connectivity **IDP Reference # n/a**	60 000	60 000	60 000	60 000	240 000
Develop an ICT Maintenance plan. **IDP Reference # n/a**				120 000	120 000
Collective Totals:	**545 000**	**945 000**	**545 000**	**765 000**	**2 800 000**

Table 51: 5 Year Implementation Plan Budget, Year 2.

11.3.3 Budget - Year 3

This section provides full view of the final-cycle-year related to the five (5) year implementation plan(s).

Official 5 Year Implementation Plan Budget: YEAR 3					
Identified ICT Initiatives	**2019 – 2020**				
	Q1	**Q2**	**Q3**	**Q4**	**TOTAL**
End User Computer Refresh **IDP Reference # SO. 8**		300 000			300 000
Develop Public Engagement App. **IDP Reference # SO. 2 - SO. 5 - SO. 9**				200 000	200 000
Implement CCTV with analytics **IDP Reference # SO. 4 - SO. 12**				1000 000	1000 000
Enhance system and network security **IDP Reference # SO. 1 - SO. 2**	62 500	62 500	62 500	62 500	250 000
Establish a fully functional Desktop Support Services **IDP Reference # SO. 1**	72 500	72 500	72 500	72 500	290 000
Upgrading of Local area network (LAN) **IDP Reference # n/a**		50 000			50 000
Upgrading of Wide Area Network (WAN) **IDP Reference # n/a**	150 000	150 000	150 000	150 000	600 000
Upgrade Internet Connectivity **IDP Reference # n/a**	60 000	60 000	60 000	60 000	240 000
Collective Totals:	**345 000**	**695 000**	**345 000**	**1 545 000**	**2 930 000**

Table 52: 5 Year Implementation Plan Budget, Year 3.

11.3.4 Budget - Year 4

This section provides full view of the final-cycle-year related to the five (5) year implementation plan(s).

Official 5 Year Implementation Plan Budget: YEAR 4					
Identified ICT Initiatives	2020 – 2021				
	Q1	Q2	Q3	Q4	TOTAL
End User Computer Refresh **IDP Reference # SO. 8**		300 000			300 000
Implement Public Wi-Fi Service **IDP Reference # SO. 2 - SO. 4 - SO. 5 - SO. 9 - SO. 11**	900 000	900 000	900 000	900 000	3 600 000
Implement CCTV with analytics **IDP Reference # SO. 4 - SO. 12**				1 000 000	1 000 000
Establish a fully functional Desktop Support Services **IDP Reference # SO. 1**	72 500	72 500	72 500	72 500	290 000
Upgrade Internet Connectivity I **DP Reference # n/a**	60 000	60 000	60 000	60 000	240 000
Upgrading of Local area network (LAN) **IDP Reference # n/a**		50 000			50 000
Upgrading of Wide Area Network (WAN) **IDP Reference # n/a**	150 000	150 000	150 000	150 000	600 000
Collective Totals:	**1 182 500**	**1 532 500**	**1 182 500**	**2 182 500**	**6 080 000**

Table 53: 5 Year Implementation Plan Budget, Year 4.

11.3.5 Budget - Year 5

This section provides full view of the final-cycle-year related to the five (5) year implementation plan(s).

Official 5 Year Implementation Plan Budget: YEAR 5					
Identified ICT Initiatives	2020 – 2021				
	Q1	Q2	Q3	Q4	TOTAL
End User Computer Refresh **IDP Reference # SO. 8**		300 000			300 000
Implement Public Wi-Fi Service **IDP Reference # SO. 2 - SO. 4 - SO. 5 - SO. 9 - SO. 11**	900 000	900 000	900 000	900 000	3 600 000
Implement CCTV with analytics **IDP Reference # SO. 4 - SO. 12**		1 000 000			1 000 000
Establish a fully functional Desktop Support Services **IDP Reference # SO. 1**	72 500	72 500	72 500	72 500	290 000

Upgrade Internet Connectivity **IDP Reference # n/a**	60 000	60 000	60 000	60 000	240 000
Upgrading of Local area network (LAN) **IDP Reference # n/a**		50 000			50 000
Upgrading of Wide Area Network (WAN) **IDP Reference # n/a**	150 000	150 000	150 000	150 000	600 000
Collective Totals:	**1 182 500**	**2 532 500**	**1 182 500**	**1 182 500**	**6 080 000**

Table 54: 5 Year Implementation Plan Budget, Year 5.

11.4 Critical Success Factors

For successful completion and/or execution of all identified ICT initiatives and meeting of objectives, critical success factors shall be noted as the primary driver towards strategic achievement. These items would be considered as but not limited to the items below:

1. Resource Capacitation: Adequate, confirmed and authorized funding is the core component towards delivery of initiatives.
2. Responsibility/Ownership: Identification of a product owner (champion per initiative – may be the same person for multiple initiatives) with the appropriate mandate and authorization is required to successfully drive all aspects of the initiative.
3. Measurement: Continually measuring the success of each aspect of the initiative is the baseline towards ensuring and maintaining of quality, with a suitable monitoring or measurement system being put in place upfront prior to undertaking of the initiative.
4. Program, project and risk management: Governance around these considerations need to be agreed upon and set as mechanism(s) prior to undertaking of initiatives, aiding and ensuring on delivery.
5. Senior and/or executive support: If there is no proper top-structure support, it is likely that the initiative may not be accurately identified to align with business needs, while simultaneously impacting and hindering on delivery of any initiative that may have been accurately identified but delegated without any proper support during the lifecycle of the initiative.
6. Ongoing engagement: Ensuring that the initiative is always aligned to the objectives of the municipality, continual reviews should be scheduled on a regular basis whether it be ad hoc or at milestone points. Reviews will ensure there is no deviation towards completion of the initiative.

12 Lifecycle and Management

The lifecycle of the ICT strategy is noted as a period of five (5) years, whereas the lifecycle of the implementation plan(s) is noted as a period of five (5) years. In context around both lifecycles, this document will be reviewed by authorized and mandated management and/or municipal stakeholders on an annual basis.

Review of the entire context of this document as a strategic document through its initiatives, legislation, alignment or orchestration shall be realigned as found best suitable to any drives of change. Should there be multiple drivers of change due to impact of legislation, regional or national initiatives or any transversals impacting on change within a single-year-period, then the latest revision of this document may be noted as the official strategy towards the remainder of the lifecycle(s).

Through the above, it may be noted that the annual review of this document will not be the only initiator to any potential change of its context or content, as other drives may dictate towards the review of it.

13 Conclusion

The Municipalitiy is positioned for success, beginning with the development of this ICT Strategic Plan, starting with the Municipal Council's Vision and objectives followed by the ICT Vision, IT Mission, and Initiatives, which provide a roadmap for future ICT investments. Through the strategies of consolidation, standardization, and simplification, the Municipality can realize a fundamental shift from continued operational spending to new project delivery.

The next step in the strategic planning effort is to develop detailed implementation plans that identify specific actions, schedules and timeframes, and resource requirements such as staffing and funding for the projects identified in the Plan.

The IT Strategic Plan is the result of a collaborative encompassing the strategic objectives of the Municipal Council. The success of this Plan is dependent upon that collaboration and the commitment of all Municipal departments. The initiatives selected are those that are most critical to achieving the Municipalities specific goals as set out in the Integrated Development Plan (IDP) and in order to align with goals as set out in the National Development Plan (NDP) and provincial goals.

The ICT Department endorses the Plan and is committed to providing the leadership and support needed to ensure successful completion of the initiatives and projects and establishing a solid technology platform that will serve as a foundation for the future.

The strategic objectives set by Council has been brought in line with ICT initiatives in order to use ICT`s as a strategic enabler in order to assist and support the objectives set out herein.

The strategic Municipal goals supported by the ICT strategic and implementation plan is as follows:

1. To create a culture of good governance
2. To create a culture of public participation and empower communities to participate in the affairs of the Municipality
3. To create an administration capable of delivering on service excellence.
4. To create an enabling environment for economic growth and development
5. To promote tourism in the Municipal Area
6. To provide effective financial, asset and procurement management
7. Provision of equitable quality basic services to all households
8. To maintain infrastructure and undertake development of bulk infrastructure to ensure sustainable service delivery.
9. To provide community facilities and services
10. Development of sustainable vibrant human settlements
11. To promote social and youth development
12. To create and maintain a safe and healthy environment

14 Annexure A: e-Governance

There are various considerations that define the makeup known as e-Governance. Below we will review and provide context to the various sections around e-Governance, while additionally providing insight into a strategy for successful application of services/systems/solutions embodied within it.

'e-Governance' is the use of ICT to enhance the efficiency of work and improve service delivery in order to meet the needs of the public in a responsive and transparent manner. E-Government is expected to facilitate the interaction between the Government and its clients including the citizens (G2C) and business communities (G2B), as well as within the public administration itself (G2G).

Expected e-Government Strategy

In summation, e-Government is expected to be delivered through four (4) phases; (a) digital presence, (b) interaction, (c) transaction and (d) transformational. Below we review the items in more detail:

1. Digital Presence: This phase will involve simple provision of government information through electronic means. Through this, government organisations will be expected to be providing one-way information and limited interaction to their clients.
2. Interaction: In this phase, Government organizations are expected to be able to use ICT to provide some degree of online interaction with their clients. For instance, citizens can be able to enter requests, complaints, or online applications, and expect to obtain an appropriate response. In this stage, secure transactions such as financial or confidential transactions that require a high degree of security-clearance authorization and audit capacity are not expected. However, the nature and capacity of each government organization/department will determine the degree of sophistication in each service provided.
3. Transaction: This phase is characterised by the provision of secure transactions through high-level authorization. Government organizations are expected to be able to provide capabilities and features that will allow clients to complete their transactions in full without the necessity of visiting Government offices. Such services may also allow the Government to function in a 24/7 mode. Typical examples may include one-stop online centres for citizens to apply for passports, permits or licenses, enabling them to make payments online.
4. Transformation: In this phase government organisations are expected to have been well joined and working together at various levels. The achieving of this stage will allow Government clients to interact with one Government instead of individual Government organizations. This phase requires collaboration to bring together suppliers, consumers and the whole government itself into a seamless network focussed on increasing value creation.

Extended Consideration

Diversification towards an e-Citizen engagement platform would be a primary focus area for government. There are citizen-side technologies that may be leveraged to the benefit of e-Governance such as computers, mobile devices, the Internet, Smart Television, Applications, and many others in enhancing delivery of services. Therefore, alignment to exploit such technologies to enhance its relationship with citizens should be a primary objective. Through the four (4) phases identified above, it provides context and suggests ways in which this intent of diversification to e-Citizenry may be achieved.

15 Annexure B: Innovation

Strategic Innovation is a holistic, systematic approach focused on generating beyond-incremental, breakthrough or discontinuous innovations. Innovation becomes "strategic" when it is an intentional, repeatable process that creates a significant difference in the value derived from it, often through means of disruption. A Strategic Innovation initiative generates a portfolio which is created using a disciplined yet creative process.

Expected Innovation Strategy

The Strategic Innovation framework weaves together seven (7) dimensions to produce a portfolio of outcomes that drive growth:

1. **A managed innovation process:** Combining non-traditional (out the box thinking) and traditional approaches (governed and procedural) to business strategy.
2. **Strategic alignment**: Building support services/systems catered towards the innovation.
3. **Industry foresight**: Understanding emerging trends and forecasting applicability of the innovation.
4. **Consumer/customer insight**: Understanding articulated and unarticulated needs.
5. **Core technologies and competencies**: Leveraging and extending corporate assets.
6. **Organizational readiness**: The ability to take action.
7. **Disciplined implementation**: Managing the path from inspiration to business impact.

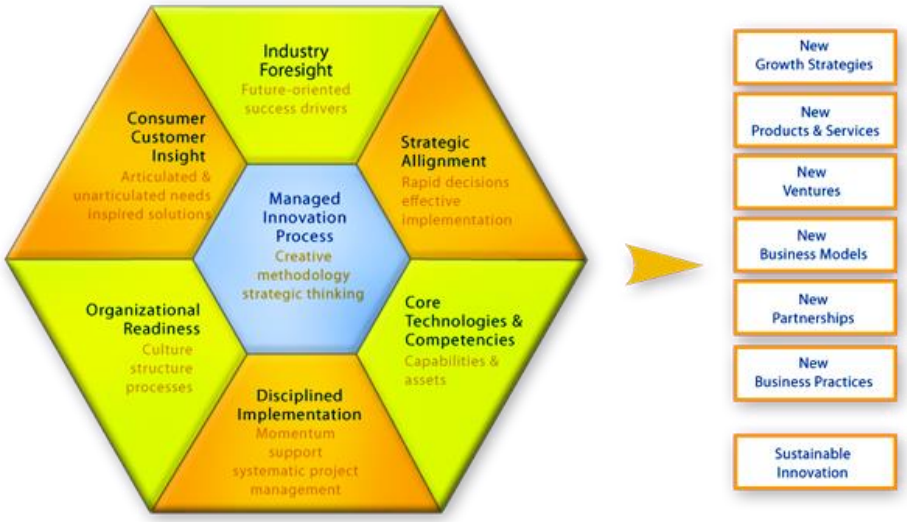

Figure 7: Strategic Innovation Framework.

A managed Innovation Process covers a sequence of activities from the beginning of an initiative through to its implementation. This provides the baseline as a catalyst to an *'all-things-possible'* perspective that demands radical rethinking, challenges the status quo and calls for critical thinking from all key stakeholders.

Extended Consideration

As a team-based framework, the approach would include workshop sessions related to; information exchange, part exploration, part mediation, part creative invention and part improvisation. These sessions stimulate cross-functional teams to look beyond the obvious and to explore and speculate about future possibilities. The workshops intentionally juxtapose unlikely, contradictory perspectives, which inspire new thinking and force a creative tension that stretches the mind to new levels of inventiveness. The resulting view of the future is then supplemented with the usual methodologies and analysis found in traditional future planning concepts.

16 Annexure C: Product Sourcing

In a concise and specific manner related to the municipality's ICT department, environment, as well as towards strategic enablement of the municipality through ICT, product sourcing should be conducted through understanding of the items all noted below.

Expected Product Sourcing Strategy

As a primary framework, a successful strategy is where sourcing has considerations related to:

1. Total Cost of Ownership (TCO): Focusing on the total and full cost related to the purchase whereby the total cost incorporates the needs of the customer, the goals of the municipality, as well as the market conditions. Internal and external factors for support/enablement need to be considered around TCO.
   Note: Purchases should not only therefore focus on the cost of the purchase by itself, as the holistic cost of ownership of the product may be far more than a better product or service as noted in point 2.
2. Best Product/Service: It is expected that the best value is to be derived from what is purchased, related to longevity as well as operational and functional support included in the cost to ensure timeous response in event the product/service becomes faulty or unstable. A Next Business Day (NBD) response-time should be the bare minimum for consideration, as a user or system/service/platform should not be down for more than 24 hours at a worse case scenario in the municipality. Therefore, only reputable vendors with a history of or referenced Service Delivery should be considered as part of any Tender Specification(s), ensuring this ties into adequately meeting the objective of successfully managing TCO.
   Note: This is a direct consideration that could hinder operations, whereby a purchase should not look at the cheapest product/service, but rather look at the business around that product/service to define if it will be a short-term purchase or drive a long-term objective. A short-term cheaper purchase may define that the business needs to realign its ICT around the cheaper purchase in a few years when the business requires something more expansive, with total cost of migrating the platform then costing more than purchasing a better product/service from the onset, which is scalable both up and out.
3. Driven Collaborative Approach: Purchases should not negate the fact when an expected purchase is to be undertaken where the item is not easily interoperable with an existing ICT platform already in place. This tied into the aforementioned points 1 and 2 define a consideration to be undertaken where Collaboration, Best Product/Service, as well as TCO be aligned closely to ensure collaboration and interoperation of ICT.
   Note: Strategic sourcing is not achieved when it is only surrounded by ad-hoc activities and not only involving purchasing.
4. Levered Savings: Purchases are to consider extended items where the purchase is all encompassing, as at times a product/service may be purchased whereby the 'up-sell' of other extended services on the platform ends up increasing costs down the line significantly.
   Note: Purchases should understand the full product/service suite related to all 'up-selling' considerations before concluding any purchases.
5. Analysis and Understanding: Decisions should consider fact based analysis and market intelligence from an internal perspective. An external party or third-party may not have the best interest or holistic understand around the long-term applicability of the product/service in both the environment itself as well as the business.
   Note: Decisions should not be based on opinions, unjustified preference or complacency.

The above components should be noted as Critical Success Factors towards conclusion for successfully sourcing of any product or service required by ICT and/or the municipality.

17 Annexure D: Service Delivery

Service Delivery within Information and Communications Technology (ICT) is related to a manner in which ICT is delivered considering its design, development, deployment, operation and lifecycle management. Operational capability is a critical component to why Service Delivery is required; the municipality both needs to not only be operational, but more so capable of operating in an optimal manner.

18 Expected Service Delivery Strategy

There are various types of Service Delivery and/or Service Management components related to successful delivery; however, the items below are to be considered as the primary components:

1. **Service Culture:** This is a primary consideration and at the forefront of Service Delivery, specifically to be understood that there is a duality to Service Culture which collectively contributes to delivery. Firstly, internal culture needs to be geared through leadership, habits, vision and values, which enable internal stakeholders to understand what is required. Secondly, an external provider/party/stakeholder who is responsible for undertaking, facilitating or concluding what is required of them to meet the expectation/request of the internal stakeholder. Through this and the quality of Service Culture both internally and externally, it enables that delivery may be experienced for being both effectively communicated around its requirements, as well as being understood on what is expected.
2. **Service Quality:** There are various components to this, but it ultimately comes down to making informed decisions around the quality of the service (product/platform/system/solution/etc.), not just related to the immediate value it may potentially bring, but more so if there would be extended value over a measurable period of time, contributing to a successful TCO Model – see Annexure C.
3. **Service Experience:** It would be a critical component towards Service Delivery that the support experience to the client or end user is as effective as possible. Engagement requiring any Service Delivery request should be minimal from the client or end user side, whereby what is required by them may be easily and adequately understood, logged, and loaded to whichever system by the party providing the service, catering for an effective turnaround time. Therefore, all items put in place within the municipality around ICT should cater for a high Mean Time To Repair (MTTR), through it being sourced/secured/provided by parties who have the according capability to ensure a timeous MTTR.
4. **Service Performance:** Through the aforementioned MTTR; all ICT components related to Service Delivery should be documented in a central location. This IT Service Delivery Document will contain all particulars related to processes, contact details, and expected turnaround time for ICT in totality. Therefore, successful Service Performance related to Service Delivery would be dictated through it being understood how MTTR is to be expected/achieved. It needs to be defined whether the undertaking would be via; an internal perspective, from an external perspective, or a combination of both.
5. **Service Results:** The results experienced through the various aspects of Service Delivery should additionally be documented alongside a Service Performance section. This will not only ensure that performance can be measured, but more so ensuring that results are captured over a period of time and reviewed quarterly, whereby it may then be compared for TCO. This will define the true value of the service.
6. **Service Consolidation:** A successful Service Delivery Strategy ultimately contains consideration whereby there is a Single Point of Contact (SPoC) supporting multiple services, instead of a provider/vendor/partner, per service. Consolidation is where MTTR and TCO to enable delivery meet.

The six (6) Service Points above will enable the municipality to manage Holistic ICT Service Delivery Strategy.

19 Appendix A: Figures

20 Appendix B: Tables