NORTHERN CAPE DEPARTMENT

OF

DEPARTMENT OF TRANSPORT, SAFETY AND LIAISON

INFORMATION TECHNOLOGY

STRATEGIC PLAN

2017/21

DOCUMENT CONTROL

Document Details

Province	Northern Cape
Document	IT Strategic Plan
Document Name	Department of Transport, Safety and Liaison Draft Strategic IT Plan Edited.docx
Document Number:	Version 1
Document Status:	Draft
Customer Contact:	053 830 1780
Customer Reference:	Thembekile Aaron
File Location:	Department of Transport, Safety and Liaison
Author(s):	Thembekile Aaron

Revision information

Revision Number	Revision Date	Change Reference
1.0	August 2018	Initial Document
		MPAT 1.7 Planning Guideline

Document Approval

Name	Designation	Signature	Date	Approval (Y/N)
M. P. Dichaba	**Head of Department**		28/11/2017	Y

LIST OF ABBREVIATIONS

AD	Active Directory
AV	Antivirus
CCR	Cluster Continuous Replication
CD	Compact Disc
COMSEC	Communications Security
COTS	Commercial Of The Shelf
CSIRT	Computer Incident Response Team
DC	Data Centre
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IDS	Intrusion Detection System
IP	Intellectual Property
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	Internet Security Acceleration
iSCSI	Internet Small Computer Interface
IT	Infrastructure Technology
ITIL	Information Technology Information Library
ITSM	IT Service Management
KPI	Key Performance Indicator
LAN	Local Area Network
MOM	Microsoft Operations Manager
NDS	Novell Directory Services
NIC	Network Interface Controller
NLB	Network Load Balancing
OS	Operating System
OU	Organisation Unit
POP	Point Of Presence
PST	Personal Storage Table
RAM	Random Access Memory
SAN	Storage area Network
SARS	South African Revenue Services
SLA	Service Level Agreement
SMS	System Management Server
SQL	Structured Query Language
TOGAF	The Open Group Architecture Framework
TRM	Technical Reference model
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WSUS	Windows Server Update Services

INDEX

EXECUTIVE SUMMARY

This ICT Strategy supports existing core Departmental goals, set in the Department of Transport, Safety and Liaison Strategic Plan of 2015/16 and 2019/20and is based on the Outcomes / Outputs:

- All people in South Africa are and feel safe
- Spatial imbalances in economic opportunities are addressed through expanded employment in agriculture, the build programme and densification in the metros.
- Maintenance, strategic expansion, operational efficiency, capacity and competitiveness our logistics and transport infrastructure ensured.

Each programme, sub programme and departmental entity has its own business strategy to deliver specific services and commitments. The ICT Strategy provides a standardised, flexible and efficient ICT infrastructure to enable delivery of these individual business objectives. It provides public servants with the confidence that they can deliver their objectives effectively and securely in a sustainable manner. Above all, it reduces inefficiency, replication of systems and duplication of effort.

The strategy will also transform ICT procurement, giving Accounting Officers the confidence that they can use services available across the public sector which have already met procurement legal requirements and provide value for money to their business. This will be assured through supply management which covers government procurement of ICT products and solutions.

The governance structure, meanwhile, ensures that information assurance (IA) requirements are incorporated into all aspects of the strategy. This will provide assurance to Risk Management and Departmental Security Management that solutions meet mandatory public sector information assurance and security requirements.

Most importantly, the strategy will enable delivery of government objectives, while maintaining local control over delivery and personalisation for services that are unique to the Department.

1. INTRODUCTION

The Department of Transport, Safety and Liaison here invests in Information Technology to support the department's purpose to create an enabling environment for economic growth and economic development in the Northern Cape Province. In order to realise this purpose, the department must achieve the following five strategic outcomes required of it by the government:

- Support and ensure the smooth functioning of the Department.
- Transparent and accountable law enforcement agencies in the Northern Cape by 2020.
- A safe and secure environment in the Northern Cape by 2020.
- To enable and ensure effective, efficient and safe mobility in the Northern Cape Province.
- To reduce road crashes and fatalities on the road by 2019 through effective promotion, coordination and implementation of road traffic strategies and legislation and to further enhance the overall quality of road traffic service by promoting, coordinating and implementing road traffic safety and by managing the process of vehicle registration and licencing.

These are underpinned by strategic priorities for the Department including:

1. **Administration:**
   To provide strategic, financial, organisational and administrative support services to the line functions of the Department.

2. **Civilian Oversight:**
   To exercise oversight functions with regard to law enforcement agencies in the Province.

3. **Transport Operations:**
   To enable and ensure effective, efficient and safe mobility in the Northern Cape Province.

4. **Transport Regulations:**
   To ensure the provision of a safe road environment through regulation of traffic on public roads, law enforcement, the implementation of road safety campaigns and awareness programmes and the registration and licencing of vehicles and drivers.

Fundamental to achieving the strategic outcomes and priorities for the department are enabling capabilities that include ICT. The ICT capability for the department includes the hardware (servers, desktops), software (email, Records Management, Custom-Based Developed Solutions) and support services (help-desk, planning) that are required to provide ICT services for the department's staff, clients and partners. Our ICT services are critical to our staff, clients and partners to support efficient access to the department's services and support our staff to meet our legislative and record keeping requirements.

The IT Plan is a small but crucial element in the Department since it deals with the alignment of Business strategy with IT. The IT Plan will give an overview of the use of IT in Directorates, with recommendations giving direction to future IT developments in the Department.

This deliverable will specifically indicate the gaps of the current Information Technology environment in support of the operations environment, and it will identify the way forward.

The IT Plan can therefore be seen to highlight any changes necessary in the Information Technology environment and associated processes of the Department, to better meet new and/or continuing governmental business needs.

1.1 PURPOSE OF ICT PLAN

The purpose of the IT Plan is to optimize the current Technology Capabilities from the current basic level to a standardized and in some cases a rationalized level, as well as addressing the highlighted challenges. This will ensure that IT adequately supports the provincial government business. Being at a standardized and ultimately at a rationalized level will achieve the following benefits;

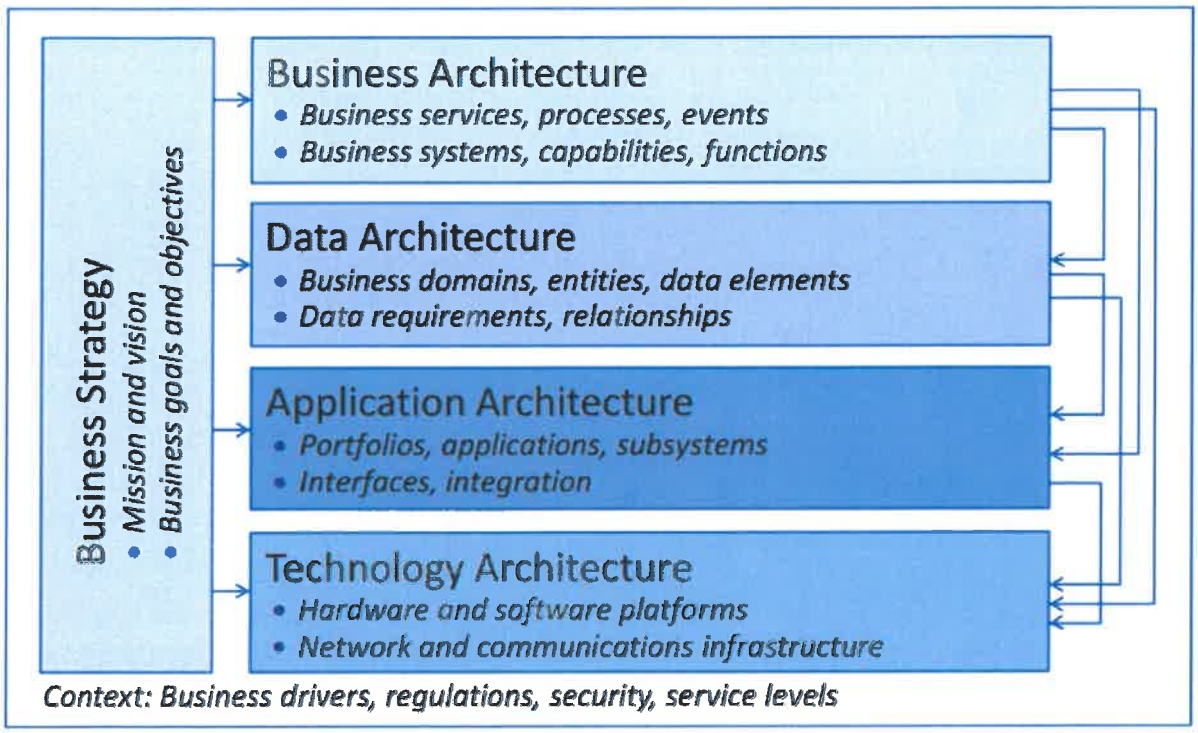
- Enforced policies and standards with consistent management and reporting services;
- Standardised Desktop and Server images and automated deployment;
- A standardised Governance Framework;
- Back-up and recovery of all Business critical systems and a well-tested Disaster Recovery solution;
- A standardised messaging and collaboration platform;
- A well-defined security standards and secure access control.

1.2 Architecture Approach

An internationally recognised enterprise architecture method (TOGAF 9) has been selected to represent the current state and to design the future state of IT in the Department of Transport, Safety and Liaison. The Enterprise Architecture is aligned to and will support the Departmental Strategy and Vision.

The current iteration of this plan focus on the technology architecture:

- **Technology Architecture** –depicts the technology solutions deployed within the Department



The vision and scope for this iteration of the future state technology architecture has been defined. In addition, a set of principles has also been adopted to govern the definition and implementation of the future state technology architecture.

The approach comprised four main phases: to document the current environment, to define the future view, to establish the gaps and to address these gaps in a roadmap over a 3-year period.

1.1 Architecture Scope

Approximately 80% of all information technology requirements are common and human efforts in maintaining and supporting the infrastructure and software are being duplicated across the eleven Northern Cape Provincial Government Departments.

For any business application to function and perform well, an infrastructure with optimised hardware and software, sufficient capacity and the latest technologies are required. This includes efficient operational and systems management, adequate tools and effective governance procedures.

In taking cognisance of this, a decision was taken to focus the IT Plan on the 80% of the Information Technology Services Stack that is common to the Northern Cape Provincial Departments and would have the biggest impact in terms of cost savings and operational efficiency.

The Data Architecture and Application Architecture domains have been excluded from this iteration of the IT Plan.

1.2 Architecture Vision

The goal of this IT Plan is to define a conceptual architecture that would form the basis for detailed architectural designs to assist departments with their acquisition, integration and development of technology. The conceptual architecture and detailed designs will define the technology blueprint for provincial departments. The solution will deliver common services through a centralised shared services infrastructure.

1.3 Guiding Principles

The following guiding principles and goals have been adopted to govern the future state conceptual architectures.

1.3.1 Business Principles

The process of development planning that gives rise to the Northern Cape Provincial Growth and Development Strategy and programmes should be guided by the following principles:

- **Equality** – notwithstanding the need to advance persons previously disadvantaged, development planning should ensure that all persons are treated equally
- **Efficiency** –the promotion of the optimal use of existing physical, human and financial resources
- **Integration** – the integration of spatially coherent regional and local economic development and improved service delivery systems
- **Good Governance** – the promotion of democratic, participatory, co-operative and accountable systems of governance and the efficient and effective administration of development institutions
- **Sustainability** – the promotion of economic and social development through the sustainable management and use of natural resources and the maintenance of the productive value of the physical environment
- **Batho Pele** – the placement of people and their needs at the forefront of its concern and serve their physical, psychological, developmental, economic, social and cultural interests equitably.

In addition to the Northern Cape Provincial principles, the following principles have been adopted to assist in guiding the technology architecture to be defined:

- **Primacy of Principles**: These principles apply to all departments within government. The only way we can provide a consistent and measurable level of quality information to decision-makers is if all departments abide by these principles

- **Protection of Intellectual Property**: The governments' intellectual property (IP) must be protected. This protection must be reflected in the IT architecture, implementation and governance processes. All systems should integrate to the government's shared authentication and authorisation procedures;
- **Protection of Investment**: New systems and infrastructure should leverage off existing government investments as far as possible provided that this does not have an impact on quality.

1.3.2 Data Principles

The following data principles were adopted:

- **Data is an** Asset: It has value to the Northern Cape Provincial Government and is managed accordingly
- **Data is Shared**: Users have access to the data necessary to perform their duties; therefore, data is shared across government functions and departments in a complete, correct and consistent form
- **Data is Accessible**: One of the benefits of an architected environment is the ability to share across the province
- **Data Security**: Data is protected from unauthorised use and disclosure. In addition to the traditional aspects of national security classification, this includes but is not limited to protection of pre-decisional (work-in-progress, not yet authorised for release), sensitive, source selection-sensitive and proprietary information.

1.3.3 Application Principles

The following application principles were adopted:

- **Common applications are shared across government departments**: The sharing of applications that are designed to enable common business processes/functions of government radically improves the economy of IT investments across government. Sharing of common applications reduces the burden of maintaining several configurations of the same type of applications, complexities in support contracts and commensurate licensing fees;
- **Ease-of-Use:** Applications are easy to use – the underlying technology is transparent to users, so they can concentrate on tasks at hand
- **Flexibility:** Applications must be implemented so that they are flexible and can adapt to changing business and legislative needs.

1.3.4 Technology Principles

The following technology principles were adopted:

- **Control Technical Diversity**: Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments i.e. limiting the number of supported components simplifies maintainability and reduces costs

- **Interoperability and Integration**: Software and hardware should conform to defined standards that promote interoperability and integration for data, applications and technology
- **Shared Services**: All common services should be offered to departments on a shared services platform
- **IT Capacity**: The infrastructure capacity must be adequate to handle governments' present and future needs
- **Enterprise Security:** The infrastructure must provide an easy, reliable and uniform means of user authentication across business functions
- **Optimised:** Technology and processes should be implemented in such a way as to make optimal use of resources (people and infrastructure)
- **Shareable:** Infrastructure and technology should be shared across all departments to the benefit of the province as a whole
- **Service Management:** Standard technical services such as security and systems monitoring must be used so that these functions are performed in a consistent manner with standardised output
- **IT Service Management:** IT Service Management should be provided for centrally and be shared across all of the departments
- **Central data centre hosting:** All servers and services will be hosted centrally in the data centres. Exceptions are to be assessed based on localised user numbers and possible performance enhancements
- **Virtualisation:** Where possible, virtualisation technology should be used allowing as many workloads as possible to be hosted using virtual machines (VMs) instead of physical servers.
- **Services and systems design**: All services and systems should be designed for high availability, scalability and be highly secured.

2. BUSINESS OBJECTIVES

2.1 **Organizational Structure**

The department has been organised along four (4) programmes as summarised in the diagram below:

We only have a hard copy of the Organogram of the Department.

2.2 Organizational Composition | Strategic Objectives

PROGRAMME 1	STRATEGIC OBJECTIVE
ADMINISTRATION	To provide strategic, financial, organisational and administrative support services to the line functions of the Department.
SUB-PROGRAMME	
1.1. Policy and Planning	• To effectively manage Departmental Compliance Planning, Reporting and Performance Information.
1.2 Office of the Chief Financial Officer	• To ensure Departmental financial compliance through financial management services over the 5 year period.
1.3 Corporate Services	• To ensure the overall corporate support and provisioning of human capital.
PROGRAMME 2	
CIVLIAN OVERSIGHT	To exercise oversight functions with regard to law enforcement agencies in the Province.
SUB PROGRAMME	**STRATEGIC OBJECTIVE**
2.1 Policy and Research	• To conduct research on policing to influence policy changes.
2.2 Monitoring and Evaluation	• To monitor and evaluate SAPS in adhering to statutory requirements and to determine and enhance the status and compliance and service delivery at police stations.
2.3 Safety promotion	• Provide integrated crime prevention initiatives for safer communities.
2.4 Community Police relations	• To strengthen relations between communities and Police.
PROGRAMME 3	
TRANSPORT OPERATIONS	To enable and ensure effective, efficient and safe mobility in the Northern Cape Province.
SUB PROGRAMME	
3.1 Transport Services	• The management of integrated land transport contracts to provide mobility to the commuters.
3.2 Infrastructure Planning	• To provide for integrated planning and coordination of intermodal facilities, transport policies and statutory plans for all modes or transport.
3.3 infrastructure operations	• To oversee and monitor the development of transport

	terminals.
3.4 Transport safety and compliance	• To manage, coordinate and facilitate transport safety and compliance for public transport.
3.5 Operator licence and permits	• The management and control of registering of transport operators and the issuing of all licences and permits required in terms of legislation.
PROGRAMME 4	
TRANSPORT REGULATIONS	To ensure the provision of a safe road environment through regulation of traffic on public roads, law enforcement, the implementation of road safety campaigns and awareness programmes and the registration and licencing of vehicles and drivers.
SUB PROGRAMME	
4.1 Law enforcement	• To improve law enforcement on Provincial roads through high visibility operations.
4.2 Road safety education	• To conduct wide scale road safety education and awareness initiatives in the Province.
4.3 Transport administration and licences.	• To provide effective and efficient law administration, licencing and ensure compliance monitoring services in the Province.

2.3 Catalogue of services

SERVICE	DESCRIPTION
• Support and ensure the smooth functioning of the Department.	• To provide strategic, financial, organisational and administrative support services to the line functions of the Department.
• Transparent and accountable law enforcement agencies in the Northern Cape by 2020. • A safe and secure environment in the Northern Cape Province by 2020.	• To exercise oversight function with regards to law enforcement agencies in the Province.
• To enable and ensure effective, efficient and safe mobility in the Northern Cape Province.	• To plan, regulate and facilitate the provision of public transport services through cooperation with the National and Local Authorities, as well as the private sector in order to enhance the mobility of all communities particularly those currently without or with limited access.
• To reduce road crashes and fatalities on the roads by 2019, through effective promotion, coordination and implementation of road traffic strategies and Legislation and to further enhance the overall quality of road traffic service by promoting, coordinating and implementing road traffic safety and by managing the process of vehicle registration and licencing.	• To ensure the provision of a safe road environment through the regulation of traffic on public roads, law enforcement, the implementation of road safety campaigns and awareness programmes and the registration of and licencing of vehicles and drivers.

2.4 ICT Objectives

The ICT Objectives of the Department

- Focusing on the development of ICT as an economic sector to build domestic capacity
  - Developing a core ICT network infrastructure

- Focusing on ICT as an enabler for socio-economic development
  - Enhancing access to sector specific information

The Department further aims to provide and effective IT Management and Administrative support service to the core Business Divisions within the Department through continuous refinement of organizational strategy and structure to ensure compliance with applicable legislation [public service act / SITA Act] an appropriate best practices to furthermore :

1. Promote a culture of customer focus in all ICT structures;
2. Identify a long term, sustainable and accessible solution that addresses increasing demands for storage and the integration and interoperability of our ICT systems;
3. Enable capacity to meet increasing network bandwidth demands and reduce single points of failure that would threaten the availability of network connectivity;
4. Create additional business efficiencies, whilst improving service quality through centralisation of core ICT provision, reducing duplication and the complexity of multiple systems and services where these exist at local level;
5. To provide universal access to broadband (as defined by the national broadband policy) for citizens, business as well as government institutions.
6. To build the Network Infrastructure and Information Super-highway to encourage the development of advanced workforce with better ICT skills;
7. To enhance economic productivity through ICT infrastructure development in order to lower the cost of doing business and increase connectivity for companies especially SMMEs
8. To Increase the ICT skills capacity within the public and the private sectors to create a pool of ICT practitioners and entrepreneurs
9. To improve service delivery by providing high quality ICT services through e-government
10. To build an economic and industrial sector with a focus on ICT, and in particular, software industry
11. To ensure that innovation becomes part of the economic network in Northern Cape Province in relation to ICT
12. To reduce the carbon footprint of the province through Green ICT
13. To create employment in the ICT sector

3. STATEMENT OF STRATEGIC INTENT

The Department has prioritized a set of strategic goals that would make the vision a reality and enable the mission statement. Targets are set for each of the Departmental strategic goals required to achieve economic growth and social development in the Northern Cape.

The Departments has to deliver and improve on mandated services provided to their customers. These services could be provided by either manual or automated processes. ICT solutions and services would be required to automate the required business functions. In doing so various types of interactions with Vendors and Suppliers are required for the acquisition of services, hardware and software, in addition to the core departmental IT team.

Interactions and exchange of information is also required between government departments and with service providers. This would assist in keeping abreast with improved business strategies in the various sectors, latest technologies and new ways of organising functional areas and resources.

Implementing some of these worldwide trends and strategies could contribute towards an improved provincial strategy and implementation thereof. In turn this would achieve:

- Improved Frontline Service Delivery [E-Government],
- Improved front / back-office functions, management practices and governance.
- Better customer service and service delivery;

The functional area within the Department may or may not align to the organisational structure. These functions are required for them to operate their business and to deliver the services they are mandated to perform.

The business capabilities selected as the focus for the development of this IT Plan are highlighted in the Figure below, viz. the Business Support Capabilities and ICT Capabilities. These support capabilities have to be supported by the future state technology architecture, which is described as part of this Departmental IT Plan.

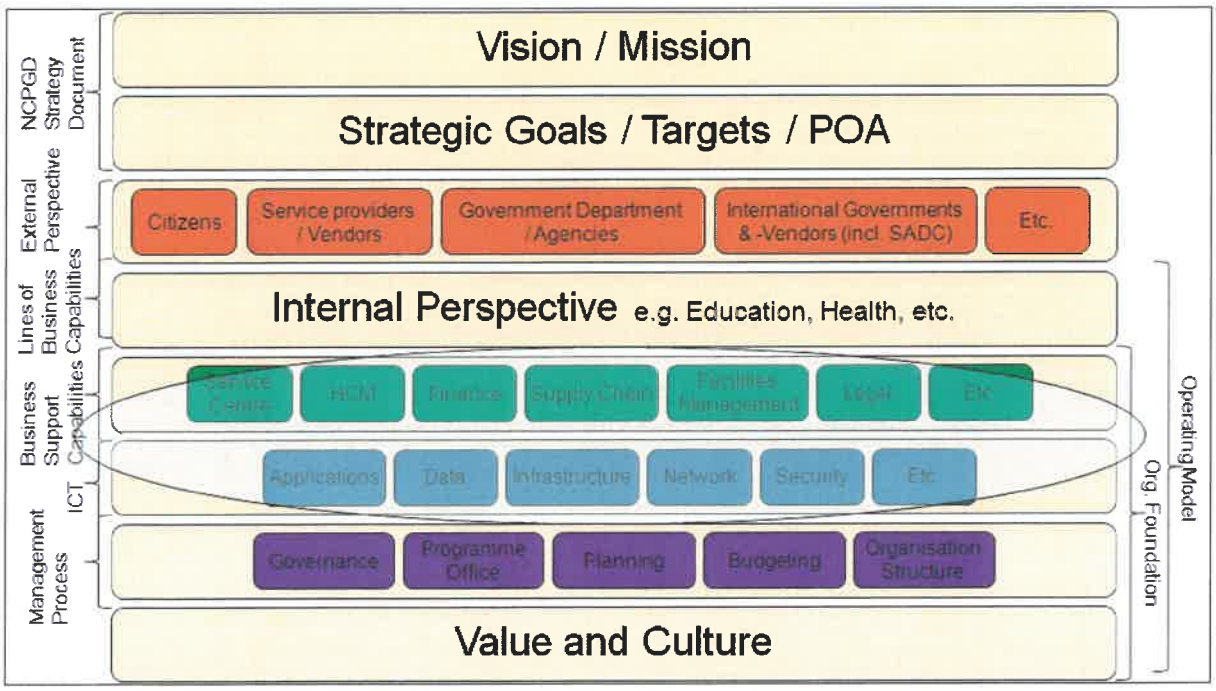


Figure 1: Scope of the Business Capabilities

These functions support departmental divisions in the execution of their line of business functions. Examples of these functions are: administration and management of finance, management of the facilities, recruitment of human resources and administration of personnel functions, procurement, asset management, legal administration and cases, etc. The support functions and related processes are common across each of the Northern Cape Province Government Departments.

The Departmental Employees execute on administrative functions on a day to day basis, to fulfill their responsibilities for a specific role within a Department. The functions is to compile and publish required letters, memo's and documents, send and receive of e-mails and faxes, schedule meetings, telephone interactions, etc., this contributes towards collaboration and knowledge share between the various employees within the business environment.

A governance framework is required within the province with the related committees, processes, policies and standards implemented for all the levels of the provincial business in terms of planning, budgeting, organizational structure and execution of the business functions. Together with this solid management practices, processes and procedures are required for the management of the daily ICT activities, incidents and problems as well as changes and new releases of hardware and software into the environment.

A Departmental project management office is required to execute, monitor and control the prioritised and funded initiatives in the Department. This office should adopt an appropriate methodology, compile the necessary processes and procedures, acquire supporting tools, and employ knowledgeable skilled resources.

Collectively all of the business support functions, processes, standards, skilled resources and supporting tools shall assist the department to execute on its mandate and to fulfil its strategic goals in its mission to provide;

- Strategic Leadership;
- Economic and Social development, and growth to the citizens of South Africa; and
- Opportunities for the poor to share partake and enjoy what the province has got to offer.

The achieve this the Departmental IT Plan aims to centralize, simplify and standardize the business support- and enabling capabilities, rather than having scattered, unique and complex support and enabling hardware and software solutions, where duplication and lack of skilled resources are prevalent.

As ICT cannot implement its objectives in isolation of the business requirements and its participation, it is necessary that the strategic objectives and the ICT objectives must be evaluated by the strategic management of a department in order to formulate a statement of strategic intent. This statement of strategic intent must include three specific areas of business service delivery:

3.1 Frontline Service Delivery [E-Government]

Government to Citizens (G2C)	Government to Business (G2B)
- Website [GCIS Website Development Guidelines] - Tourism information, - Consumer Protection - enquiring about and paying traffic fines; listing - government services offered, - grade 12 and education results, past matric - papers, schools search and online registration, - e-learning - online learners and drivers booking system, - vehicle license enquiries, - animal disease monitoring, - schedules of public transport - e-grants and e-vital such as identity - documents, birth registrations and passports	- Supplier Registration and Querying - Tendering Publication and Application, - Online support portal for SMMEs -
Government to Government (G2G)	**Intra-governmental: Internal efficiency and effectiveness**
- Provincial Geographic Information System (Provincial Intervention) - disaster response management - Share and integrate provincial and municipal data - e-legislation(rules), -	- online HR policies and procedures, - leave balances and application, - e-records management, - Directory of Services - Call Desk / IT Helpdesk - Resource Management - Document Management - Enterprise Content Management Systems - Email Services - Supply Chain Management - e-recruitment, - e-learning/training, and -

3.2 Back Office and Supporting

- Database Management
- Human Resources - Persal
- Financial Management– BAS
- Budget Tool
- E-Channel
- E-Disclosure
- MPAT Portal
- Assets/Materials Management - LOGIS
- Development and Integration
- E-Recruitment
- E-PMDS
- Electronic Records Management

- Enterprise Content Management
- Software Development
- Database Development
- Web design and development

3.3 Interdepartmental Cooperative Requirements

- ICT Infrastructure [SITA Next Generation Network]
- Shared Email [Novell Groupwise]
- Shared Server and Virtual Shared Server Operations
- Help Desk / Desktop Support
- Shared Software Solutions
- Shared Antivirus Solution
- Shared Directory Services
- Windows Update Services (WSUS)
- Business Continuity Management

4. VISION

[Vision indicating that ICT must enable business in the execution of its mandate,]

'A fully fledged Knowledge Economy in the Northern Cape wherein the Information Society harnesses the evolution of ICT and ensures that knowledge creation, sharing as well as information manipulation become the engine for economic growth and development'

The vision is interpreted through the following Goals:

- **Goal 1 Productivity:** To create a heightened environment for ICT-enabled economic activity amongst large firms and SMEs; for electronic government services to citizens and business; and for support measures for ICT research and development (R&D).
- **Goal 2 Connectivity Networks**: To foster the diffusion of ICT fixed and mobile broadband infrastructure and the connectedness of SMMEs, schools and households, in ways that contribute to reducing the cost of communications and, therefore, of economic participation.
- **Goal 3 ICT skills Capacity**: To address the demand for skills in the broad ICT infrastructure and ICT services sectors, as well as in the society at large; and to provide for online learning in every primary and secondary school classroom; as means to increasing South Africa's future competitiveness and laying the foundation for ICT innovation and sector development

5. MISSION

5.1 Mission statement

"IT Services will be recognised as an innovative and influential function, playing a core role in the operation and ongoing development of the Department.

5.2 ICT Business Enablement Objectives.

Delivering the ICT that the business needs for Departmental and District Office working will require a number of key ICT enablers, each providing key functionality to teams across the Department and its District Offices.

Desktop and Telephones

- All Departmental Offices support flexible working, but currently with different desktop and phone strategies. These will be aligned over time.
- The relevant desktop, laptop and mobile phone equipment will be given to Departmental working staff, wherever they may be working. The councils will ensure the telephone networks are able to easily redirect numbers across the three networks, including public facing numbers so that flexible estate management and moving teams between locations does not require public facing numbers to be changed.

Sharing Documents and Emails

- Staff working in different districts will need to access single email solution.
- Document sharing will be delivered through a single shared collaborative area.

Phone and Web Conferencing

- District Offices will need to communicate efficiently across a wider range of locations, without having to lose time travelling. Fast and effective phone and web conferencing facilities need to be in place.

Access to Applications and Information

- Shared access to applications and information will be delivered through the Next Generation Network (NGN) framework agreement, together with re-engineered security arrangements.

Application Consolidation

- The Department will prioritise application consolidation in line with business need and ability to deliver savings, taking account of contract expiry dates, including sharing applications across services (for example, creating intranet and internet sites in the same system), and common applications from single suppliers where possible.

Information Governance

- Access to information and continued ownership of information assets across the re-organised services will be crucial for Tri-borough working.

- A Departmental Information Management Strategy and Information Governance model will be developed, ensuring correct information sharing and compliance with Data Protection and Freedom of Information Acts.
- A new security model will be required, with protection built around applications and data rather than the current high security perimeters, using a mixture of encryption, inherently secure computer systems, and data level authentication. The security model will consistent with the standards required by the secure public sector network shared between local authorities and other government organisations.

Approach to Customer Services

Delivering a transformed approach to customer services may involve, in accordance with sovereignty on service provision, a range of opportunities for:

- Sharing a single Interactive Voice Recognition (IVR) platform, implemented in the most customer friendly way possible, to provide economies of scale savings and consistent functionality across the councils, with council specific branding to reflect each council's sovereignty.
- Jointly developing e-Government (mobile and web) capability across the Department, and an understanding of the costs of different channels to drive future service development.
- Enabling greater mobile access to relevant applications for both customers and staff, including secure information access and transfer without staff needing to return to the office.

6. PERFORMANCE INDICATORS

There are no ICT Strategic objectives in the Strategic Plan of the Department.

7. ICT BUSINESS ENABLEMENT

7.1 PRIORITIZED 5 YEAR ICT BUSINESS ENABLING SOLUTIONS ROADMAP

[Enter your Departmental Services and Related e-enabled services here (Use your Departmental Service Charter as baseline for services– Delete this note After Completion]

Institutional business objective	Institutional programme and function responsible for the objective	Name of business service	Name of business owner of the service	Name of business enabling ICT initiative	Purpose of the ICT initiative	Value criteria	Measure for value item
Related objective as reflected in the institutional strategic plan;	Name of the institutional programme and function responsible for realising the objective and the name of the executing function as per the institutional strategic plan;	Name of the business service as per the institutional catalogue of services;	The line or staff function official tha-t ultimately owns and is responsible for the service being delivered;	The general name that the user community uses to refer to the business enabling technology either as an individual ICT element (i.e. e-mail) or a collective name (i.e. IFMS);	Description of the purpose of the business enabling ICT initiative;	Definition of the value criteria (see Annexure A);	How the institution will go about to measure whether value was realised;

Name of business service	ICT objective (i)	New/ Existing initiative (j)	Annual mile-stones and MTEF budget				
			YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
Name of the business service as per the institutional catalogue of services;	Description of the ICT objective the initiative will realise over the next 5 years;	Indicate if it is a new initiative or continuance of an existing initiative.					

8. Stakeholder Analysis

[Institutions should perform internal and external stakeholder analysis with regards to the ICT enablement of service delivery and describe in line with the following Table]

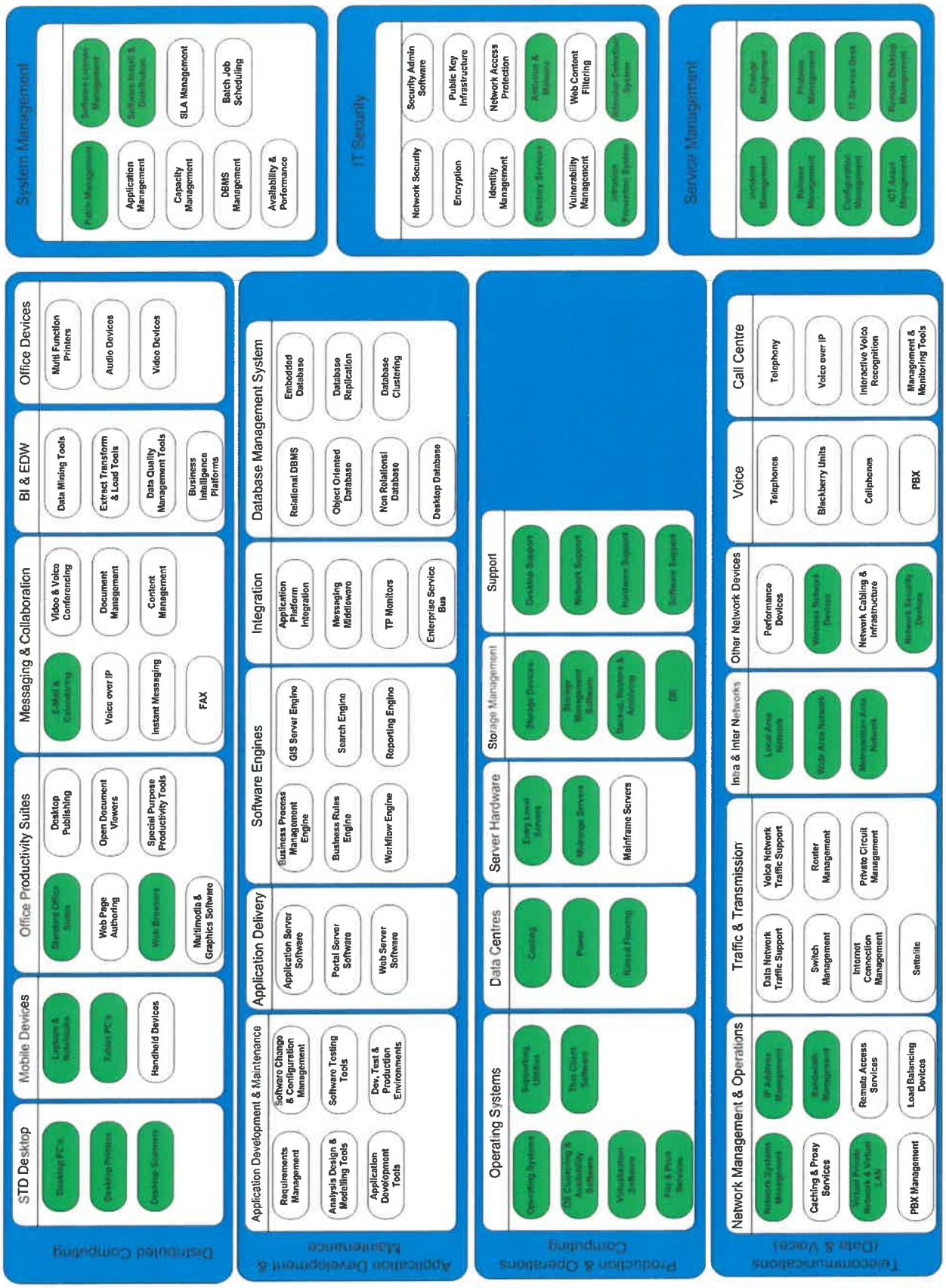
Stakeholder **(a)**	**Role of the stakeholder** **(b)**	**Influence** **Indicate High (H), Medium (M) or Low (L)** **(c)**	**Importance** **Indicate High (H), Medium (M) or Low (L)** **(d)**	**Impact** **Indicate High (H), Medium (M) or Low (L)** **(e)**	**Mitigation** **(f)**
List internal or external stakeholder as at the time of the development of the plan;	Define the role of the stakeholder;	Indicate the influence the stakeholder has on realizing this plan;	Indicate the importance of the stakeholder in terms of his/her/its role in achieving the plan;	Determine and indicate the impact of the non-cooperation of the stakeholder; and	Depict mitigation measures where relationships are not on par with what is required.

9. TECHNOLOGY ARCHITECTURE,

9.1.1 Technology Standards Catalogue

Name	Description	Date	Category	Source	Created/ Amended	Standards Class

9.1.2 Technology Reference Model



Technical Reference Model

A model that defines the major classes of technology components/services (infrastructure software, hardware, and network) and the interoperability standards associated thereto.

The TRM contains technology elements that should be present in the Northern Cape Provincial IT environment. Selected elements within the Infrastructure Domain, Messaging and Collaboration, Security and Endpoint Device Management sections of the TRM will be addressed as part of the IT Plan.

Table 1: Common IT Service Groups

IT Services Groups	IT Services
Distributed Computing	Standard desktop
	Mobile devices
	Office productivity suites
	Messaging and collaboration
	BI and EDW
	Office devices
Application Development and Maintenance	Applications development and maintenance services
	Application delivery
	Software engines
	Integration services
	Database management system
Production and Operations Computing	Operating systems
	Data centres
	Server hardware
	Storage management
Telecommunications (Data and Voice)	Network management and operations services
	Traffic and transmission services
	Inter and intra data centre network services
	Other network devices
	Voice network services
	Call centre services
IT Security	Physical environment services
	Identification, authentication, authorisation services
	Detection, response, recovery, audit services
	Perimeter defence services
System Management	System management
Service Management	Service management

These services could be provided to departmental users from a shared services data centre. The services selected to form part of the shared services landscape listed per IT Services Group include:

Table 2: Shared / Localized Service Components

Service Group	IT Service	Service Component
Distributed Computing	STD Desktop	
	Mobile Devices	Laptops and Notebooks
	Office Productivity Suites	Standard Office Suites
		Web Browsers
	Messaging and Collaboration	e-Mail and Calendaring
Application Development & Maintenance	Out of Scope	
Production & Operations Computing	Operating Systems	
	Data Centres	
	Server Hardware	
	Storage Management	
	Support	
Telecommunications (Data and Voice)	Network Management and Operations	Network Systems Management
		IP Address Management
		Bandwidth Management
		VPN and VLAN Services
	Intra and Inter Networks	
	Other Network Devices	Wireless Network Devices
		Network Security Devices
IT Security	Antivirus and Malware	
	Directory Services	
System Management	Patch Management	
	Software Licence Management	
	Software Install and Distribution	
Service Management	IT Service Desk	

Remote Desktop
Management

Profile of common IT Services

Distributed Computing

Distributed Computing Services includes the provision and support of workstation hardware (i.e. PCs and notebooks) and the set of capabilities that support office productivity suites, email and calendaring, browsers, anti-virus and common utilities, etc. This service group also provides the capabilities that support work group communications, corporate administrative and programme-specific applications, directory services, file and print services, remote access services, local network operating systems, locally attached peripherals and the local interconnectivity provided through Local Area Network (LAN) technologies.

- The IT Services included within this section are: Standard Desktop, Mobile Devices, Office Productivity Suites, Messaging and Collaboration.
- The IT Services excluded are: Office Devices, BI and EDW. Refer **Error! Reference source not found.** to view the Service Components included (in green) and excluded from this IT Plan.

Standard desktop, mobile devices and office productivity suites

What does it do: New desktop devices (i.e. PCs and notebooks) come fully set up with a standard suite of basic software. They are ready to use with an operating system and a web browser. Email and calendaring software are made available on these devices as part of a productivity suite to the departmental users.

Why do we need it: Desktops are required by employees within a department to execute on their daily activities and responsibilities, such as using word processors and spreadsheets and accessing business applications, intranet and Internet; scheduling meetings and sending emails electronically, to mention but a few.

Table 3: STD desktop, mobile devices and office productivity suites current and future view

[current state findings and the future state recommendations for Standard desktop, mobile devices and office productivity suites services.]

Desktop, Office Suites	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure	Standardised desktop brands, models Standard policy and procedures are deployed.	Standardised desktop brands, models and productivity office suites that make it easier, quicker and cheaper for the departmental IT units to maintain them and to support the users.
Technology	Limited standardisation of office productivity suites exists within the Department Standard user profiling is lacking across the board, resulting in more expensive and diverse licensing models.	Standardised office productivity suite software throughout the Department Standard images should be in place for the roll out of new desktop devices or the re-build of faulty devices. An enterprise licensing agreement should be in place for use by all departments in the province. Standardised user profiles should be in place for all desktop users.
Support	Centralized Desktop Support	The support personnel should be skilled and certified in the supported technologies. Automated usage policies and commissioning and decommissioning of procedures should be in place.

Note: Instances of remote support software will be installed for technical support staff. Security access and audit policies will be enforced via directory services policies.

E-Mail and Calendaring

What does it do: Email is a method of communication where digital messages are exchanged across the Internet or other computer networks. Email servers accept, forward, deliver and store messages. Organisations depend on email as one of their *de facto* forms of communication.

Why do we need it: Email systems are required to provide secure and reliable enhanced communication. We require them to operate in a managed and secure environment with a low cost of ownership.

Table 4: Email and Calendaring current and future view

[current state findings and the future state recommendations for the email and calendaring services.]

Email	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure		All server components should be hosted centrally centres with replicated redundancy between the two sites for each critical component including mail transport and mailbox storage.
Technology	GroupWise 6.5 and 7	The Department should standardise on a single email platform.
Support	Centralized Departmental Support	Users should be profiled according to their requirements and categorised as heavy, medium or light. Skills required to support this environment should be part of a centralised team. The support personnel should be skilled and certified in the supported technology. Policies and procedures should be in place and should include mailbox size limits, send\receive limits, deleted item retention periods based on user profiles. Policy based mailbox management should be implemented to effectively manage the available messaging resource utilisation.

Note: 6 000 users' roles should be split. Dedicated virtual servers should be allocated for transport/.filtering, mailbox and client access. There should also be a split of approximately 1 500 users per mailbox server.

The Roadmap section can be referenced for the initiatives required to be implemented in order to bridge the gap between the email current and the future state.

Application Development and Maintenance Services

Application Development and **Maintenance Services** includes the provision and support for application development services that create new or enhanced functionality in support of programme-specific and corporate/administrative services (e.g. finance, material, human resources). Application Development and Maintenance Services provides the set of capabilities that support all hardware, software and services related to applications development, maintenance, testing, and transfer to Production and Operations Computing services for pre-production and production operations. Including, for example, operating system(s), tools, languages, compilers, databases, training aids, test and development servers, peripherals particular to the development and maintenance environment, development and maintenance of custom web applications, custom-built applications, and customised front ends and testing of commercial off-the-shelf (COTS) enterprise applications (e.g. SAP, PeopleSoft, RDIMS, etc.).

We deliberately excluded Line of Business applications in departments as highlighted in the scope section. This section needs to be developed in a later iteration of the IT Plan.

Production and Operations Computing Services

The Production and Operations Computing Services includes the provision and support for the enterprise's day-to-day operations, production application system and database computing environments, including web application hosting environments, regardless of where they reside in the enterprise (centralised or within departments). In addition, this service group enables web-hosting environments within the intranet, Internet, and extranet environments.

The IT Services included in this section are Operating Systems, Data Centres, Server Hardware and Storage Management. All of these are being addressed within Data Centres. Refer to **Error! Reference source not found.** to view the Service Components included (in green) and excluded from this IT Plan.

Data Centres

What does it do: Data centres cover the centralisation and consolidation of common service infrastructure and software into a secure managed location. Key functions also include appropriate location, physical security, environmental components like power and cooling. The operations of a data centre contain enterprise management tools and a skilled support team.

Why do we need it: Operations, infrastructure and application services would be fully integrated and common hardware, software and services would be leveraged. Duplication of effort and cost would be reduced and efficiencies in terms of the availability, management and support would be improved. Provincial Government Information, which is our most valued asset, would be maintained and secured centrally. Technologies such as virtualisation can also be leveraged.

Table 5 contains the current state findings and the future state recommendations for the data centre services.

Table 5: Data centres current and future view

Data Centres	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure	The Department owns and manages a separate server infrastructure for its own systems and applications.	All servers and operating systems should comply with predefined standards. A Cold, Warm and Hot Disaster Recovery solution should be in place. Business continuity should include centralised storage, clustering, data replication etc.
Technology	Most systems and applications are deployed and hosted on multiple servers in multiple locations. The software is often out-dated utilising mixed models and versions. Software support contracts and SLAs are often not in place. Technologies such as virtualisation are not utilised.	Common software components should be consolidated and standardised. Software should be refreshed to the latest versions. A backup tool should be in place for use by all departments.
Support	Critical data is not being backed up. Centralized Departmental Support	Services should be delivered from a central location Support personnel within the Department should be consolidated providing focused and improved management and service delivery for the whole province.

Error! Reference source not found. contains the data centre environment hardware components that were identified for the Northern Cape Province shared services environment.

The Roadmap section can be referenced for the initiatives required to be implemented in order to bridge the gap between the Data Centres current and the future state.

Telecommunications (Data and Voice)

The Telecommunications Network services group includes both data and voice services. Data network services include the provision and ongoing support of multi-platform, multi-protocol electronic data and communications networks, which includes all software as well as wiring, switches, hubs, routers and all other hardware required to support data communications between computing devices. The voice communication or unified communication services includes the provision of local and long-distance services , as well as fax services, voice mail, video-conferencing, instant messaging, secure voice over internet protocol (VOIP) and other related services, which include all carrier software and hardware environments.

The IT Services included in this section are: Network Management and Operations Services, Traffic and Transmission Services, Inter and Intra Data Centre Network Services, Other Network Devices and Call Centre Services. The IT Services excluded are: Voice Network Services. Refer to **Error! Reference source not found.** to view the Service Components included (in green) and excluded from this IT Plan.

IT Security

IT Security Services is concerned with applying "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information".

The IT Services included within the IT Service Group for this iteration of the IT Plan are: Physical Environment Services, Identification, Authentication, Authorisation Services, Detection, Response, Recovery, Audit Services and Perimeter Defence Services. Refer to **Error! Reference source not found.** to view the Service Components included (in green) and excluded from this IT Plan.

The security policy, guided by ISO 27002 deals with 12 components. This document, however, only looks at two elements, namely Antivirus and Directory Services. Network security is dealt with in the Network Management and Operations section of the document.

Antivirus and Malware

What does it do: Viruses can come in all forms and have different effects. Some collect information, while others install malicious software, otherwise known as malware or spyware onto personal computers. Viruses can be picked up by using a peer-to-peer sharing programme, opening an email attachment, or loading music into your computer from someone else via a USB flash drive or even a burned CD. Many viruses are hard to detect. Spyware and malware both are very good at disguising themselves and have evolved into serious threats. Many of today's viruses have evolved to a point where they are capable of taking down large networks. Anti-Virus software protects PCs from being infected by these virus outbreaks

Why do we need it: Having virus protection is important, but just as important as the virus protection itself, is keeping the virus protection program updated. Viruses, adware, spyware and malware are created and released into the wild every single day. Security firms keep those virus definitions updated as quickly as possible to ensure that contamination is contained. Antivirus

software should be deployed to do daily updates of all PCs in the environment, to protect and counter potential threats.

Table 6 contains the current state findings and the future state recommendations for the antivirus and malware services.

Table 6: Antivirus and Malware current and future view

Antivirus and Malware	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure	The antivirus infrastructure is centralised within the department.	The antivirus infrastructure is centralised within the department.
Technology	The antivirus technology within department is predominantly Kaspersky Endpoint protection version 10.	Define and implement an IT Security Policy and Blueprint.
Support	Support is done at a departmental level.	The support personnel should be skilled and certified in the supported technology.

Systems Management

Systems Management Services is the enterprise-wide management of IT systems. This discipline includes Patch Management, Service Level Management, Availability Management, Capacity Management, Business Continuity Management and IT Security Management. This document only looks at Patch Management. The other elements will be addressed in later iterations of the IT plan.

Patch Management

What does it do: Patch management helps to maintain a healthy and secure network by providing and controlling security and system patches centrally.

Why do we need it: Viruses and worms exploit security vulnerabilities in software to attack a computer and launch new attacks on other computers. These vulnerabilities also provide opportunities for attackers to compromise information and assets by denying access to valid users, enabling escalated privileges and exposing data to unauthorised viewing and tampering. Keeping the computing environment secure and reliable is a priority for IT departments. Failure to keep up to date on security patches (and the prerequisite service packs) can have a devastating effect on departments when vulnerabilities are exploited. On average Microsoft alone has been releasing seven to eleven critical patches and updates weekly. Multiplying that number by approximately 6 000 computers across the Northern Cape Provincial IT landscape and we see that 42 000–66 000 patches a week becomes quite a maintenance task. It is therefore important for this service is automated and maintained as part of a standard across the province. This standardised and centralised service will yield cost benefits and improve security of government systems.

Table 7 contains the current state findings and the future state recommendations for the patch management services.

Table 7: Patch Management current and future view

Patch Management	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure	Patch distribution, management and reporting are not automated. Critical and security patches, hot fixes and service packs are approved and deployed manually with little consistency and reliability. Patch and service pack deployments are not officially tested prior to deployment to ensure stability, application support and compatibility. No centralised reporting or dashboard view is available to monitor rollout success, update status and compliance across the province. The patch management infrastructure is decentralised and housed within each department.	Centralised patch management and software distribution infrastructure should be deployed for use by all departments in the province. This will provide centralised reporting and policy management. The infrastructure should cater for both Microsoft and non-Microsoft updates and custom packaged software deployment. A central update server should feed downstream proxy servers. These proxy servers should be placed at departmental district offices based user populations and bandwidth constraints.
Technology	Some departments have WSUS implemented which is not well integrated and is managed in isolation. WSUS only caters for Microsoft based patch and update management, leaving the other applications and operating systems unpatched and vulnerable. Departments handle these on a case by case basis using a manual process.	The PC lifecycle tool should cater for the entire PC lifecycle, augmenting automating inventory, software distribution, patch management including operating system deployment. WSUS forms the base patch management solution as it is integrated into the Microsoft platform and provides the core features required. WSUS should be complemented with a software distribution platform capable of customised package deployment and reporting. Visionary products on the Gartner magic quadrant include Microsoft SMS, Altiris and LANDesk.

Service Management

Service Management Services is the discipline of transforming resources into valuable services. It is an approach to effectively and efficiently deliver Managed IT Services which meet business and user expectations. Services include IT Service Desk, Incident Management, Problem Management,

Change Management, Release Management and Configuration Management. This document only looks at the IT Service Desk; the other elements will be addressed in later iterations of the IT plan.

IT Service Desk

What does it do: The IT Service Desk is the primary interface of the IT Unit. Its primary goal is to facilitate the communication, identification and the restore of critical IT services within the agreed upon service levels. It is responsible for acting as a single point of contact for the entire IT Organisation and has primary responsibilities around Incident Management, Executive reporting and providing the primary support for the business operations. Remote desktop access is software used allowing a technician to access a user's desktop remotely while the user is performing an activity so that a diagnosis of the problem experienced can be made.

Why do we need it: The IT Service Desk acts as the single point of contact for IT Service related issues and is responsible for the co-ordination and management of the Incident lifecycle, including priorities, issue referrals and escalation. It is the primary channel of communication between IT Service Providers and End Users including incident and change status reports, managing service catalogues etc. With remote desktop access the technician can make an immediate diagnosis of problems experienced by users and therefore does not have to travel long distances to make the diagnosis.

Table8 contains the current state findings and the future state recommendations for the IT Service Desk.

Table 8: IT Service Desk current and future view

IT Service Desk	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure	Currently each department has its own IT Help Desk infrastructure utilised by users to log problems, faults and incidents with the IT Service Desk agents. Users log requests by means of email, telephonically or on an ad hoc basis.	A centralised IT Service Desk should be deployed for use by all departments in the province. It should be a single point of contact for the Northern Cape Provincial Departments when problems and incidents are experienced. The necessary request logging and management software tools should be made available to all departments. Provision should be made for 1st, 2nd and 3rd line support structures, automatic request routing functionality and report back mechanisms. Various request logging channels, such as telephone, fax, email, automatic request logging, etc should be available to the users.
Technology	Spreadsheets, manual tools or in some cases, an in-house developed request	Service Management processes and procedures, i.e. incident, problem,

IT Service Desk	BASELINE (AS-IS)	TARGET (TO-BE)
	logging application is utilised by the various IT Service desk agents within the departments. The software is implemented local to the various departments with no single management view available within a department or within the Northern Cape Province for monitoring and reporting purposes. There is currently no configuration management database available for accurate logging, monitoring and control of IT related assets.	change and release management, should be integrated into the IT Service Desk systems, remote tools and monitoring functionality Requests should be logged and managed from start to finish by the IT Service Desk utilising an automated It software management solution such as Remedy. Remote access control software should be implemented for diagnosis of problems experience by the users.
Support	Limited IT Service Desk agents are available within this IT Help Desk to assist users with logging of problems experienced. Different IT support personnel are despatched from different departments to perform similar support functions in the same remote locations resulting in wasted travel and resource time. Each department follows its own problem logging and support processes and procedures	All the Northern Cape Departments service delivery technical engineers should form a central Virtual Support Team to ensure ease and a well maintained skill leveraging environment. Logged requests should automatically be routed to the first available agent, 1st Line IT Service Desk agent. If the request cannot be resolved, it should be routed to the 2nd Line Support (back-office support) or to support technicians based centrally and on-site at the larger Departments. Technicians should use the remote access software available to diagnose problems experienced.

Note: All infrastructure management and reporting would be done centrally. Service desk and technical support agents would access functions via a web interface. This infrastructure would leverage a central database backend.

We recommend that ITIL be adopted and the processes be integrated into a Configuration Management Database tool. A programme needs to be put in place to configure and implement such a tool and to skill the resources on ITIL and the IT software management tool such as Remedy.

The Roadmap section can be referenced for the initiatives required to be implemented in order to bridge the gap between the It Service Desk current and the future state.

Having a centralised hosting and operational support model as opposed to a decentralised operating model ensures the re-use of facilities, infrastructure, software, centralised budgets and an available pool of skilled resources.

The proposed solution is based on core infrastructure components that aim to do the following:

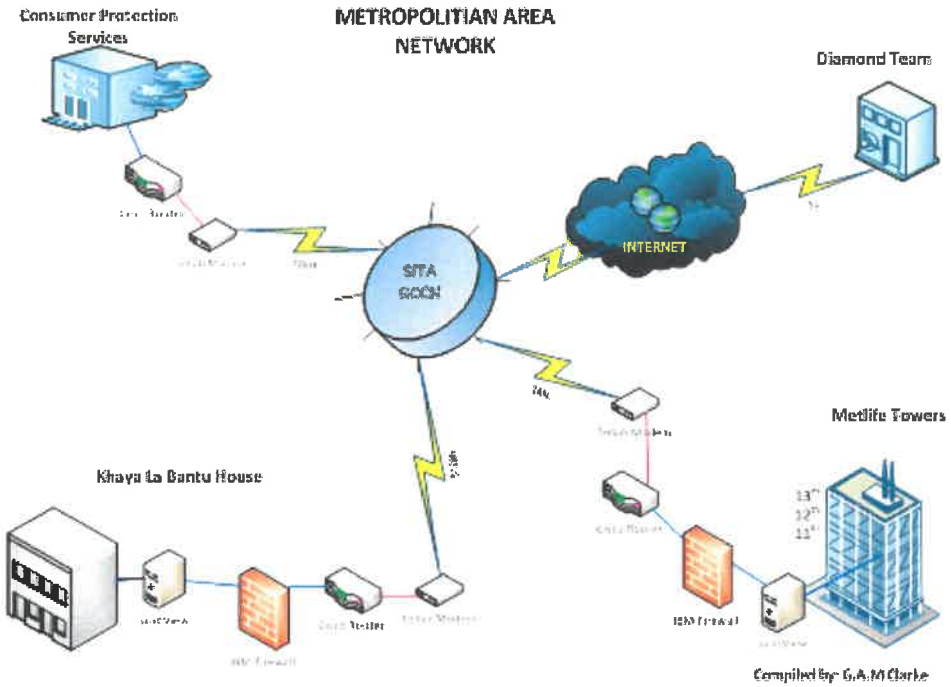
- Consolidate server infrastructure that house common departmental services like mail, directory services, antivirus etc. into two central data centres in Kimberley and Upington
- Use virtualisation technologies to minimise server and storage footprints within these data centres
- Provide a well-managed network infrastructure that is efficient, secure and cost effective
- Provide a centralised IT Service Desk to serve all departments in the province
- Provide 1st, 2nd and 3rd level IT support to all departments in the province
- Provide a Disaster Recovery capability within the province with formalised backup and restore processes and procedures
- Standardise the patch management and antivirus solutions and provide these to all departments within the province;
- Standardise desktop hardware and software and introduce thin client technology for low end users
- Provide central directory services to all departments in the province.

9.1.3 Technology Distribution Model

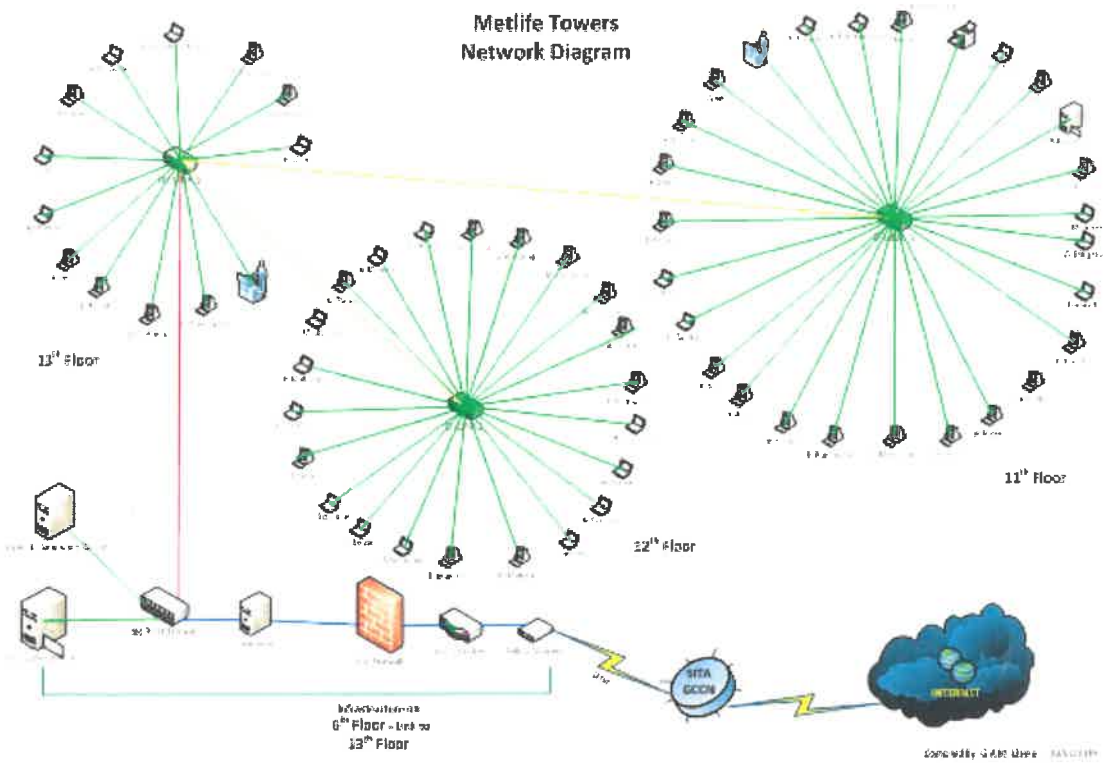
[A model that defines the technologies in different locations/environments, e.g. development environment, production/hosting environment, user environment, etc]

Format: **Nested Box Diagram** or **Network Diagram**

NETWORK - DIAGRAM



BUILDING – OCEAN ECHO



Network Management and operations;

What does it do: Managing networking systems refers to the activities, methods, procedures and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

Why do we need it: The network has to be kept up and running smoothly. Network management functions that are performed to ensure this network availability include controlling, planning, allocating, deploying, coordinating and monitoring of resources of a network.

Table9 contains the current state findings and the future state recommendations for the network management services.

Table 9: Network Management current and future view

Network Management	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure	The current Wide Area Network Services are provided and supported by SITA. Departmental LAN infrastructure does not conform to any standards or industry best practice. The lifecycle management on LAN equipment is very poor. Weekly reports are done on the health of the network which gives switch / router percentage availability statistics per department. These reports are discussed in contact sessions with departments.	Departments should have a greater level of insight into the performance and control of the WAN network. Standards for network equipment should be developed to which all new equipment acquisitions should comply. LAN equipment should be controlled using a Lifecycle management process defined for the province. All existing LAN equipment within departments should be evaluated and all unmanaged switches and hubs should be upgraded.
Technology	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed within the SITA network core. WAN network management is done by SITA using Netcool, Nethealth, HPOpenview, Ciscoworks and Netscout. Quality of Service is not optimally customised and is done on a best effort basis only.	Network virtualisation technologies such as VPN and VLANS should be deployed within the network Quality of Service should be deployed to support predictable performance for network systems. An enterprise monitoring tool should be hosted centrally and be used by all departments for management downstream.
Support	There is a shortage of skilled support personnel.	Skills required to support the network environment should be part of a centralised team. The support personnel should be skilled and certified in the supported network technologies.

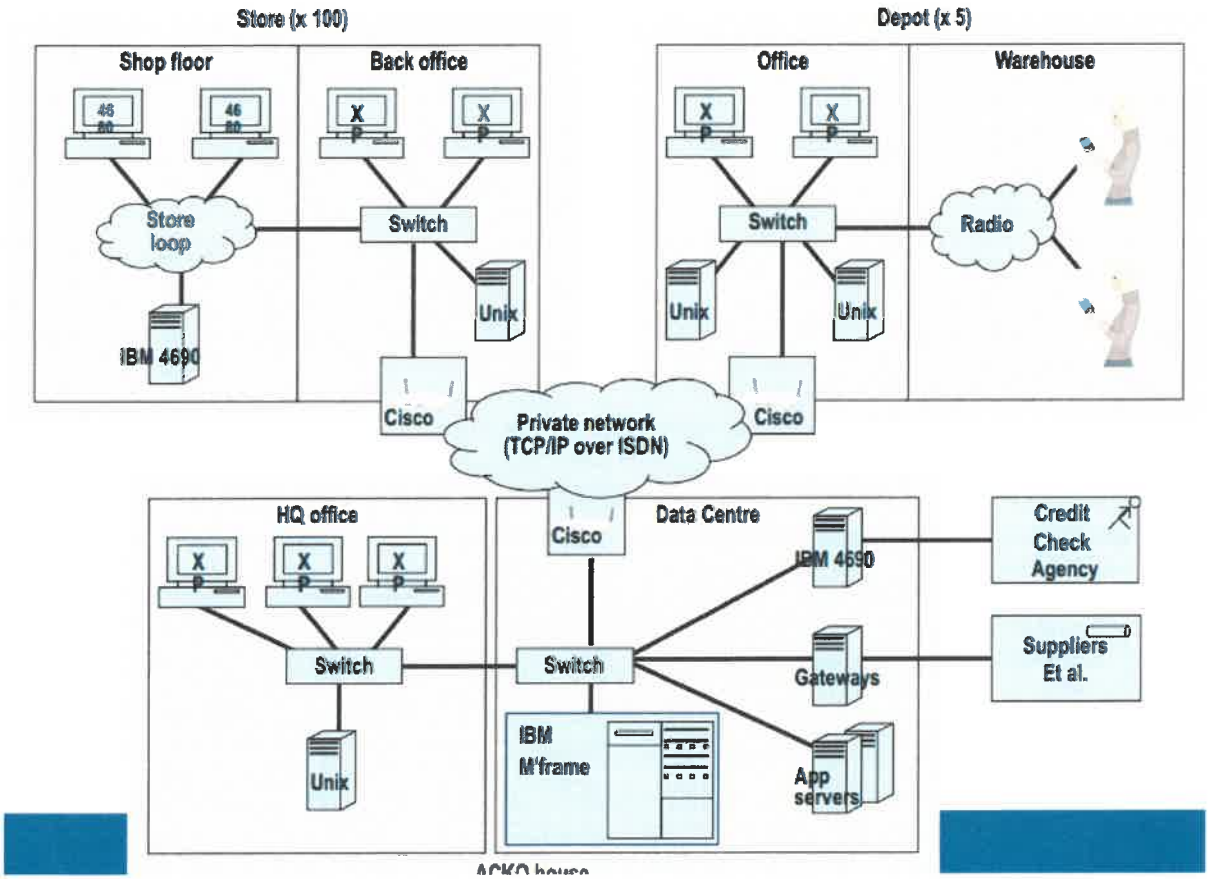
9.1.4 Technology Platform Model

A model that defines the Technologies in relation to the different subsystems in a distributed computing or client-server configuration.

Format: **Nested Box Diagram** or **UML Package**

NETWORK COMPUTING DIAGRAM

To show the "as deployed" logical view of logical application components in a distributed network computing environment.



Technology Platform Model	BASELINE (AS-IS)	TARGET (TO-BE)
Infrastructure		
Technology		
Support		

9.1.5 TECHNOLOGY GAP REPORT

[A model that indicates the deficiencies and opportunities for improvement that is derived from a comparison between the Baseline Data Architecture models and the Target Data Architecture models.]

The gaps in the technology supporting the applications and data layers of the architecture, have been highlighted as follows:

- LAN diagram – pending upgrade of network core infrastructure
- Redundant servers
- Functionality of network not optimal
- Network health assessments
- Social networking
- Building not sufficient
- Capacity management
- Backup management
- License management

	Baseline (As-Is)	Target (To-Be)	Alignment of current initiatives to Target State
None	None	None	None
None	None	None	None
None	None	None	None

9.1.6 TECHNOLOGY ARCHITECTURE ROADMAP

[A list of individual increments of change over a timeline to show progression from the Baseline Architecture to the Target Architecture.]

[Focus on Shared Services] - GET Shared Services Roadmap

Table: Programme Streams and Cost Estimates

Project	**2014/15** **R'000**	**2015/16** **R'000**	**2016/17** **R'000**	**TOTAL**
New Building Project: Data Centre\ Not Building One	None	None	None	None

New Building Project: Network	None	None	None	None
Disaster Recovery Site	None	None	None	None
Microsoft Platform Migration	None	None	None	None
IT Security Improvements	None	None	None	None
Centralized IT Service Desk	None	None	None	None
Enterprise Server Solution	None	None	None	None
iPads Project	None	None	None	None
Mobile Device Management	None	None	None	None
IT Monitoring Solution	None	None	None	None
LAN Maintenance	None	None	None	None
Backup Solution	None	None	None	None
Wireless (PTA)	None	None	None	None
TOTAL				