

Pixely Ka Seme District Municipality



Developed and Sustainable District for Future Generations

MASTER SYSTEMS PLAN (ICT STRATEGY)/ GOVERNMENT WIDE ENTERPRISE ARCHITECTURE 2022 - 2026

1 Document Properties

Attributes	Value
Project Name	Review of the Information Communication and Technology (ICT) Master Plan
Document Number	FINAL
Document Version	V1.01
Version Date	May 2022
Document Name	ICT Master Plan (GWEA)

C L

TABLE OF CONTENTS

1	DOCUMENT PROPERTIES	2
2	TABLE OF FIGURES	8
3	ACRONYMS	9
	PREFACE	11
	FOREWORD	12
	EXECUTIVE SUMMARY	14
4	SITUATIONAL ANALYSIS	15
4.1	PERFORMANCE ENVIRONMENT	15
4.1.1	<i>Strengths</i>	17
4.1.2	<i>Weaknesses</i>	17
4.1.3	<i>Opportunities</i>	18
4.1.4	<i>Threats</i>	18
4.2	DESCRIPTION OF THE STRATEGIC PLANNING PROCESS	18
4.3	GOVERNANCE ARRANGEMENTS	20
4.4	THE BUSINESS OF THE DISTRICT MUNICIPALITY	20
4.5	USE OF ICT IN THE MUNICIPALITY	21
4.6	ICT AS AN ENABLER	21
4.7	ICT STRATEGIC IMPERATIVES	22
4.8	BUSINESS VIEW OF ICT ROLE	23
4.9	PROPOSED ICT STRUCTURE	24
	CONCEPTUAL ARCHITECTURE (CA).....	26
5	INTRODUCTION	27
5.1	PREVIOUS READING	28
5.2	NOTATION AND TERMINOLOGY	28
5.3	ARCHITECTURAL REQUIREMENTS	29
5.4	BEST PRACTICES AND TRENDS	29
5.5	PRINCIPLES	29
2.	CONCEPTUAL PRINCIPLES	29
2.1	BEST PRACTISES AND PRINCIPLES	29
5.5.1	<i>BP1 Evolving a Holistic Enterprise Architecture</i>	30
5.5.1.1	PR1 Skilled Business Technologists	30
5.5.1.2	PR2 Common Vision	30
5.5.1.3	PR3 Single Corporate Planning Process	30
5.5.1.4	PR4 Visible Strategy	30
5.5.1.5	PR5 IT: Strategic Investment for Business Enablement	31
5.5.1.6	PR6 Enterprise Models	31
5.5.2	<i>BP2 Reduce Integration Complexity</i>	31
5.5.2.1	PR7 Open Standards	31
5.5.2.2	PR8 Process-Driven Business Solutions	31
5.5.2.3	PR9 Technology Standards	32
5.5.2.4	PR10 Portability and Scalability	32

M.R.

5.5.3	<i>BP3 Leverage IT</i>	32
5.5.3.1	PR11 Technology/Digital Innovation	32
5.5.4	<i>BP4 Information is valued as an enterprise asset</i>	33
5.5.4.1	PR12 Data Management	33
5.5.4.2	PR13 Information Sharing	34
5.5.4.3	PR15 Metadata	34
5.5.5	<i>BP5 Leverage BI and MIS</i>	34
5.5.5.1	PR16 PKSDM Corporate Data Positioning Guidelines	35
5.5.5.2	PR17 OLTP / OLAP Separation	35
5.5.6	<i>BP6 Unified Architecture Management</i>	35
5.5.6.1	PR18 Architectural Governance	36
5.5.7	<i>BP7 Governed Evolution</i>	36
5.5.7.1	PR19 Architecture Planning and Implementation	36
5.5.7.2	PR20 Short-term Bridging Policy	36
5.5.8	<i>BP8 Event-Driven</i>	37
5.5.8.1	PR21 Event-Driven Systems	37
5.5.9	<i>BP9 Application Re-engineering</i>	37
5.5.9.1	PR22 Granulation and Coupling of Application Systems	37
5.5.10	<i>BP10 Build for Competitive Advantage</i>	37
5.5.10.1	PR 23 "Build" or "Buy" Applications	37
5.5.11	<i>BP11 Logical Partitioning</i>	38
5.5.11.1	PR24 Logical Partitioning	38
5.5.12	<i>BP12 Messaging</i>	38
5.5.12.1	PR25 Message-Based Interfaces	38
5.5.13	<i>BP13 Enterprise Network as a Virtual LAN</i>	39
5.5.13.1	PR26 Network Interface	39
5.5.14	<i>BP14 Server Partitioning ("Workloads")</i>	39
5.5.14.1	PR27 Physical Server Boundaries	39
5.5.15	<i>BP15 Appropriate Geographic Partitioning</i>	39
5.5.15.1	PR28 Server location	40
5.5.16	<i>BP16 Virtualisation</i>	40
5.5.16.1	PR29 Virtual Data Centre	40
5.5.17	<i>BP17 Architecture Ownership</i>	40
5.5.17.1	PR30 Architecture In-Sourcing	40
5.5.18	<i>BP18 Application Programming</i>	41
5.5.18.1	PR31 Define Programmer Domain	41
5.5.19	<i>BP19 Infrastructure Re-use Development</i>	41
5.5.19.1	PR32 Infrastructure Patterns	41
5.5.20	<i>BP20 Value Add</i>	42
5.5.20.1	PR33 Value Measurement	42
5.5.21	<i>BP21 Rapid Decision-Making</i>	42
5.5.21.1	PR34 real-time access to data	42
5.6	MATRIX OF BEST PRACTISES AND PRINCIPLES	43
BUSINESS ARCHITECTURE (BA)		45
6	MANAGEMENT SUMMARY	46
7	INTRODUCTION	47
7.1	PURPOSE	47
7.2	EVOLUTION APPROACH	48

u.k.

7.3	PREVIOUS READING.....	48
7.4	NOTATION AND TERMINOLOGY.....	48
8	DRIVERS FOR BUSINESS ARCHITECTURE.....	50
8.1	ARCHITECTURAL REQUIREMENTS FOR BUSINESS ARCHITECTURE	50
	AR1 <i>Implement strategies with minimal impact on service delivery.</i>	50
	AR2 <i>Compete in a global economy according to best practices and trends.</i> ...	50
	AR3 <i>Deliver flexibly packaged and priced services</i>	50
	AR4 <i>Monitor, measure and track service delivery to clients.</i>	51
	AR5 <i>Provide controlled access to reliable and secure information</i>	51
	AR6 <i>Cost Effectiveness</i>	51
	AR7 <i>Enable good governance according to best practices and trends.</i>	51
8.2	BUSINESS PROCESSES	51
	8.2.1 <i>Core Processes</i>	51
	8.2.2 <i>Support Processes.</i>	52
8.3	CONCEPTUAL PRINCIPLES	52
9	BUSINESS ARCHITECTURE DELIVERABLES.....	52
9.1	BUSINESS MODELS.....	52
	9.1.1 <i>"The Big Picture" (Enterprise Value Network)</i>	53
	9.1.2 <i>Enterprise Value Network (EVN)</i>	53
	9.1.3 <i>Information Value Network.</i>	55
9.2	BUSINESS SCENARIOS	56
9.3	BUSINESS PATTERNS	57
9.4	BUSINESS EVENT/PROCESS MODEL.....	58
9.5	FUNCTION/PROCESS DECOMPOSITION	59
9.6	GEOGRAPHIC MODEL	60
9.7	INTEGRATION MODELLING	61
9.8	ORGANISATION ARCHITECTURE	62
	INFORMATION ARCHITECTURE (IA).....	63
10	MANAGEMENT SUMMARY	64
11	INTRODUCTION	65
	11.1 PURPOSE.....	65
	11.2 NOTATION AND TERMINOLOGY	66
12	DRIVERS FOR INFORMATION ARCHITECTURE.....	67
12.1	ARCHITECTURAL REQUIREMENTS FOR INFORMATION ARCHITECTURE.....	67
	AR1 <i>Implementing Strategies</i>	67
	AR2 <i>Workflows</i>	68
	AR3 <i>Flexibly Packaged Services</i>	68
	AR4 <i>Monitoring, Measuring and Tracking.</i>	68
	AR5 <i>Controlled Access.</i>	69
	AR6 <i>Cost Effectiveness</i>	69
	AR7 <i>Good Governance.</i>	70
12.2	INFORMATION NEEDS	70
	12.2.1 <i>Customer</i>	70
	12.2.2 <i>Geographical information.</i>	70
	12.2.3 <i>Assets/Property</i>	71
	12.2.4 <i>Human Resources</i>	71

U.K.

12.2.5	<i>Finance</i>	71
12.2.6	<i>Governance</i>	71
12.2.7	<i>Services</i>	72
12.2.8	<i>External information</i>	72
12.2.9	<i>Conceptual Principles</i>	72
13	INFORMATION ARCHITECTURE DELIVERABLES	73
13.1	INFORMATION MANAGEMENT AND CONTROLS.....	73
13.2	INFORMATION SOURCES.....	73
13.3	INFORMATION CLASSES	74
13.4	INFORMATION VALUE NETWORK.....	74
	GAP ANALYSIS	76
14	GAP ANALYSIS	77
14.1	STEPS	77
14.2	MATRIX.....	77
14.2.1	<i>Business Requirements</i>	77
14.2.2	<i>Information Requirements</i>	80
	ENTERPRISE ARCHITECTURE (EA)	83
15	OVERVIEW	84
15.1	PURPOSE AND SCOPE.....	84
15.2	DEFINITIONS.....	85
15.3	OBJECTIVES.....	85
15.4	APPLICABILITY	86
16	APPROACH AND PHILOSOPHY	86
17	INFORMATION GOVERNANCE	87
17.1	INFORMATION PROTECTION	87
17.1.1	<i>Ownership</i>	88
17.1.2	<i>Security Classification</i>	90
17.1.3	<i>Access Security</i>	91
17.1.3.1	<i>Information Access</i>	92
17.1.3.2	<i>Network Access</i>	92
17.1.3.3	<i>Remote Access</i>	94
17.1.4	<i>Business Continuity Planning (BCP)</i>	94
17.1.5	<i>Virus Protection</i>	95
17.2	INFORMATION QUALITY.....	96
17.2.1	<i>Metadata</i>	96
17.2.2	<i>Integrity/Authenticity</i>	97
17.2.3	<i>Classification</i>	99
17.3	INFORMATION MODELLING	100
18	INFORMATION MANAGEMENT ROLES AND RESPONSIBILITIES	101
18.1	INFORMATION ARCHITECTURE.....	101
18.2	DATA RESOURCE MANAGEMENT.....	103
18.3	OWNER.....	104
18.4	CUSTODIAN.....	104
18.5	USER.....	104

u n

18.6 ARCHITECTURE REVIEW BOARD.....	104
ENTERPRISE ARCHITECTURE ROADMAP.....	105
19 THE ENTERPRISE ARCHITECTURE ROADMAP.....	106
19.1 BUSINESS/ICT ALIGNMENT.....	106
19.2 DRIVERS AND OBJECTIVES	106
19.3 ICT GUIDING PRINCIPLES.....	109
19.3.1 <i>Management, Organisation and Governance</i>	109
19.3.2 <i>Applications and Information</i>	109
19.3.3 <i>Architecture and infrastructure</i>	110
19.4 GUIDING GOVERNMENT'S ICT EFFORTS	110
19.5 THE ITM-IRM-IL FRAMEWORK	112
19.6 ROLES PER ITM-IRM-IL FRAMEWORK	112
19.7 ROADMAP SEQUENCING	117
20 COMPLIANCE REQUIREMENTS.....	123
21 DISTRICT DEVELOPMENT MODEL AS PART OF ENTERPRISE ARCHITECTURE.....	125
RECOMMENDATIONS AND PLAN OF ACTION.....	127
22 RECOMMENDATIONS	128
22.1 RISK MANAGEMENT, ACTION PLANS & ESTIMATED BUDGETS	128
22.1.1 <i>Risk Management</i>	129
22.2 PLAN OF ACTION	130

U-R.

2 Table of Figures

Figure 1: Information Ecosystem.....	22
Figure 2: Ideal ICT Structure	24
Figure 3: Proposed Structure - Office of the Municipal Manager.....	25
Figure 4: Conceptual Architecture	28
Figure 5: Principles Matrix.....	44
Figure 6: Enterprise Value Networks Definition	55
Figure 7: Information Value Network Definition	56
Figure 8: Business Scenario	57
Figure 9: Business Event/Process	59
Figure 10: Function/Process Decomposition.....	60
Figure 11: Zone Modelling.....	61
Figure 12: Integration Modelling	62
Figure 13: Information Management	85
Figure 14: ICT Strategic Drivers	107
Figure 15: District Development Model	126

h R

3 Acronyms

Acronym	Full Description
AG	Auditor General
AR	Architecture Requirements
BA	Business Architecture
BP	Best Practice
BCP	Business Continuity Plan
BOB	Best of Breed
CA	Conceptual Architecture
CFO	Chief Financial Officer
CGICT	Corporate Governance of Information Communication Technology
COBIT	Control Objectives for Information Related Technology
CPM	Critical Path Method
CRM	Customer Relationship Management
CRV	Common Requirements Vision
CS	Corporate Services
DBMS	Database Management System
DDM	District Development Model
DEP CFO	Deputy Chief Financial Officer
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
ECM	Enterprise Content Management
ECT	Electronic Communication
ERP	Enterprise Resource Planning
EVN	Enterprise Value Network
EXCO	Executive Committee
GIAMA	Government Immovable Asset Management Act
GICT	Governance of Information Communication Technology
GRAP	Generally Accepted Accounting Principles
GIS	Geographic Information System
GWEA	Government Wide Enterprise Architecture
IA	Information Architecture
IAR	Information Architecture Requirements
ICT	Information Communication Technology
IDP	Integrated Development Plan
IGR	Inter Governmental Relations
IMST	Information Management Systems Technology
IP	Information Principle
IR	Information Requirements
ISO	International Standards Organisation
IT	Information Technology
IT	Information Trends
ITO	Information Technology Officer
IVN	Information Value Network
LAN	Local Area Network
LED	Local Economic Development
LOB	Line of Business
MFMA	Municipal Finance Management Act
MM	Municipal Manager

U.R.

MIS	Management Information System
MISS	Minimum Information Security Standards
MSP	Master Systems Plan
MSS	Manager Support Services
NARS	National Archives and Records Services
NAS	Network Attached Storage
PAIA	Promotion of Access to Information Act
PC	Personal Computer
PFMA	Public Finance Management Act
PGDS	Provincial Growth and Development Strategy
PKSDM	Pixely Ka Seme District Municipality
PR	Principles
ROI	Return on Investment
SAICA	South Africa Institute of Chartered Accountants
SAN	Storage Area Network
SANS	South Africa National Standards
SARS	South African Revenue Service
SCM	Supply Chain Management
SITA	State Information Technology Agency
TA	Technical Architecture
TCO	Total Cost of Ownership
TT	Technology Trends
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network

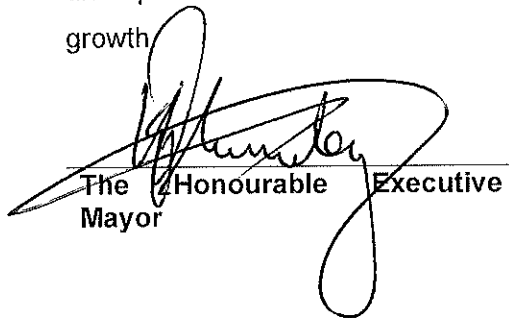
G.H.

Preface

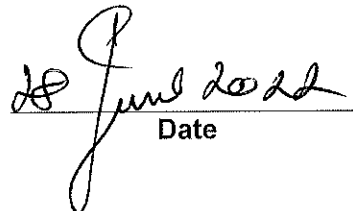
The delivery of the PGDS objectives relies on the growth of the Information Management Systems and Technology (ICT) and diffusion of ICT's in all parts of the local economy. The strategy demands an improvement in the accessibility of municipal services.

ICT is a central nervous system of municipal operations and currently accounts for a small proportion of capital expenditures within the municipality. Due to the key role played by ICT, it should be treated with at least the same due diligence as any other capital investments in the municipality. Sound business cases that support our local economic development (LED) must be created.

Optimising information technology investments is not an option, but a business mandate of the municipality, given the many opportunities for value of creation, cost savings, timelines, and accurate information that serve as seminal elements contribute towards to this mandate. Our unwavering commitment to this ICT strategy will underpin social transformation and ensure sustainable and equitable economic growth



The Honourable Executive Mayor



28 June 2022
Date

Foreword

On behalf of the PKSDM, I am pleased to present this Integrated Master Systems Plan. This is an exciting initiative for the Municipality and is directed at supporting the Municipality goals and objectives. We are well into the timeframes of the IDP, thus ICT Strategy will go a long way in supporting the municipal goals to 2026. The fourth industrial revolution is upon us and there cannot be any second guessing.

This is truly the culmination of municipal efforts towards an ICT strategic planning process. The ICT plan clearly demonstrates our vision for ICT and our understanding of the importance of a business centric approach to Information Systems and Technology investments decision-making.

We believe that ICT could play the dual role of enhancing social and economic development by acting as an enabler of service provision as well as an industry in its own right. ICT can enable PKSDM to make significant improvements in both productivity and service quality.

Through developing this integrated ICT Strategy, we have tried to ensure that the ICT initiatives have a broad reach and will deliver maximum value. This integrated ICT is the result of consultative process involving internal municipal stakeholders. We thank all those who gave time towards this large task and hope that their efforts continue to ensure the success of ICT in the Municipality. It is our desire that our endeavour to contribute to the Provincial Growth and Development Strategy.

Investment in ICT initiatives has the potential to create an Information centric enterprise where key information is well managed, available, reliable and secure. This will, in-turn, strengthen monitoring and evaluation through the availability of up-to-date information. The establishment of a project dashboard populated with accurate information per project being run by PKSDM, enabling informed decision making by Executive Management, is just one of the many benefits that will arise. Ultimately, the implementation of the ICT Plan will result in the streamlining and reengineering of key business processes and in the safeguarding of critical departmental information.



The achievement of the above requires reliable project delivery based on robust and repeatable processes, thus the focus is on the Municipality's overall investment in ICT to:

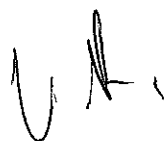
- Match ICT supply with municipal business demand;
- Identify duplication and other opportunities for standardisation and sharing;
- Develop Municipal Enterprise Architecture and ICT governance policies; and
- Measure the impact of ICT projects against the municipal ICT Strategy mission.

We are committed to implementing the initiatives we have identified in this ICT Strategy and will review our progress against the plan on an annual basis. There will be some challenges on this journey, but we will endeavour to succeed on the mission we have embraced.

Municipal Manager

Date

Executive Summary



4 Situational Analysis

The ICT unit of the PKSDM was established to provide the ICT environment, infrastructure and facilities necessary to enable and support the work of the District Municipality. With the convergence of communications and computing technologies, the opportunity arises to further these aims through the innovative application of technology. It is timely, therefore, to outline a plan to make the PKSDM a world leader in 'e-Council', improving access, communication, community engagement, improving service delivery and transparency of the work of The District Municipality and Council Members.

Underpinning much of the success of the PKSDM is a significant investment and reliance on Information, Communications and Technology (ICT). Personal computing devices are physically and geographically independent of fixed networks and they provide intuitive means of reading articles, watching videos, collaborating on projects, phoning home and video-conferencing.

The use of new digital technologies to access information quickly, utilising the pervasiveness of broadband and other networks, provides exciting options and opportunities for the PKSDM to connect, operate more efficiently and be more open to the public.

The convergence of these technologies provides the context for the delivery of the District ICT Master Plan. This plan has been developed to facilitate the PKSDM's adoption of ICT becoming a showcase example, setting an e-Council benchmark that is acknowledged both nationally and internationally.

4.1 Performance Environment

The analysis below show unit's organisational readiness to contend with the operational challenges it faces revealed that major deficits (weaknesses and gaps) exist in key performance areas, and as such, attention to these is both critical and strategic. There is an urgent need to attend to the following shortcomings:

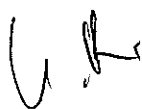
- Fill in critical vacant posts within the unit;



- Limited management of the institution's intellectual property including document management;
- ICT initiatives are not coordinated through ICT section;
- Low user confidence in ICT's ability to support business;
- Inadequate computer literacy level;
- Lack of ICT forums for users to contribute and to communicate their needs;
- Lack of user awareness on ICT Policies and procedures;
- Inadequate upskilling training for staff in the various technologies for some time resulting in staff lagging behind in capabilities to support new technologies;
- Dependence on external service providers;
- Legacy systems in use are incompatible leading to more time spend on resolving problems;
- Lack of a coordinated approach to deal with problems resulting in staff operating in silos;

In order for the IT Unit to successfully meet the external challenges identified, the unit must be properly prepared and equipped to function at optimal levels. Three performance areas were considered: Concept, Competence, and Commitment.

- **Concept** refers to *Understanding of purpose, clarity of focus, knowledge of the organisational direction and the sharing of these within the unit.*
- **Competence** refers to *The skills, abilities, talents, knowledge of staff and tools of trade within the unit.*
- **Commitment** refers to *The passion of senior management, financial support and involvement of staff.*



4.1.1 Strengths

1. There is a 2-men team with renewed vigour, energy and commitment to harnessing institutional memory and capacity;
2. The unit has enough hardware and software tools to execute its mandate;
3. There is a willingness to learn in the team and understands its shortcomings;
4. ICT Governance structures are in place putting the unit on a higher pedestal;

4.1.2 Weaknesses

1. There is a high vacancy rate and while the norm is 1:25 for each offering there is only 2 technicians at operational level as opposed to 4 required;
2. Staff have not been on upskilling training for the various technologies for some time meaning that they lag behind;
3. There is no Helpdesk facility;
4. The legacy systems in use are run solely by the vendors resulting in high expenditure;
5. The ICT Governance Committee is comprised mainly of senior managers and not business unit operatives;
6. ICT is executed at operational level rather than strategic level;
7. There is lack of a coordinated approach to deals with problems – people operate in silos;
8. Business requirements of the IT unit are not clearly articulated and communicated;
9. IT unit is wrongly positioned;
10. Network is slow during bad weather; and
11. There is no Service Charter – Operational Level Agreements with other business units.

U.R.

4.1.3 Opportunities

1. There is an opportunity to upskill staff on new technologies using the work skills plan and additional budget that can be obtained;
2. Executive management can be influenced for the adoption of new technologies;
3. The municipality can use Sage as a financial system as it is a cloud based technology system to comply with the AG's findings on offsite back up;
4. Migration to Microsoft 365 comes with lots of advantages including cloud back up, teams for meetings and security;
5. Implementing the Active Directory Service will enhance user authentication and deployment of patches automatically;
6. The unit has an opportunity to make its presence felt in the municipal environment by reversing the current negative perceptions users hold; and
7. There is an opportunity to fix everything that has not been right with of executive management support.
8. The Team can attend the GovTech annual event hosted by SITA where most new technologies are introduced and displayed.

4.1.4 Threats

1. Lack of controls may lead to unauthorised access into essential systems leading to losses;
2. Budget constraints may hamper the efforts/ability of the unit to deliver on its mandate e.g. lack of funding for Microsoft 365;
3. Lack of adequate human resources to execute IT services will impact negatively on the users;
4. Lack of buy-in from Executive management impacts negatively on the unit's ability to prioritise on critical projects;
5. The inoperation of the Disaster Recovery Plan may lead to loss of critical data and applications;
6. Conflict of project priorities may lead to undesired consequences
7. Dependence on external forces often leads to delayed decision making on key priorities;

The unit was constrained to deal with all challenges, weakness and threats because of lack of a formal strategic plan. The strategic planning sessions for the unit will from now be reviewed annually in order to update all planning and operational documents.

4.2 Description of the strategic planning process



Timeframes for planning is now consistent with Treasury Regulations and the budget and planning cycle as directed by National Treasury. The management transition during the first quarter of the year necessitated a slight delay in the process.

The unit has developed a schedule of action plans to be followed through for the next five years. The action plan take into account projects underway which had not been included in the current strategic plan.

The Unit reviewed the following documents in relation to the new strategic plan it intends to take and adopt:

- PKSDM IDP;
- ICT Strategy Plan Developed in 2019;
- AG Report;
- IT Governance Framework;
- IT Disaster Recovery Strategy;
- IT Policies;

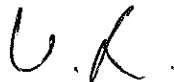
Throughout the process, a wide range of stakeholders including business departments such as Corporate Services, Infrastructure Housing and Planning and Finance were involved and consulted.

The ICT Strategic Plan outlines how ICT will enable the connection of Council Members, the public and the municipal business units to the information and services they need, building on an already solid base of using technology to support Council initiatives.

This is the District wide ICT Strategic Plan and supporting governance model to oversee the continuous development and delivery of ICT for the District.

It also:

- will be used as the basis for future ICT planning and investment, providing a sound basis for investment decisions across the municipal business units;



- outline a high level implementation plan and next steps;
- outline where efficiencies can be made and costs reduced through improved use and reuse of technology, resulting in further reduction of paper, power and travel costs; and
- will be treated as a living document that may change depending on new business imperatives or opportunities resulting from the rapid maturing or introduction of new technology.

This strategic plan will be reviewed and updated annually.

The ICT Strategic Plan is subordinate to the PKSDM's institutional IDP and provides the context of ICT planning across the municipal corporate plans.

4.3 Governance Arrangements

The PKSDM IT Specialist is responsible for the development and implementation of the ICT Master Plan. The PKSDM Governance Steering Committee (PKSDMGSC) will oversee and guide the continued development and implementation of the plan.

4.4 The Business of the District Municipality

The business of municipality can be represented in the context of the functions, roles and processes that define and support its operation.

The objective of an open, accountable, responsive and efficient Council can be more readily achieved through the utilisation of existing and emerging ICT developments including increased use of video and tele-presence capabilities and secure mobile devices.

The key internal business drivers for ICT in the Council context are outlined as follows:

- the specific business requirements of the chamber to enable the Council to function effectively;
- the requirements of the Council committees;



- facilities and support to enable individual Council Members to carry out their duties; and
- corporate and administrative support required by Council Members and by the Municipal business units.

In addition, a core driver of any ICT Master Plan in the PKSDM context is connecting the public and other stakeholders to their Municipality.

4.5 Use of ICT in the Municipality

The use of ICT in the PKSDM has been considered in the development of this plan.

The three most important improvements in the work of the Municipality made possible by ICT are:

- more information and documentation on the website;
- increased capacity to disseminate information and documents; and
- more timely delivery of information and documents to Council Members.

While these three enhancements serve Members well, they also help The District Municipality to be more open and transparent to citizens.

4.6 ICT as an Enabler

ICT enables new ways of doing business, providing the opportunity to re-think the traditional operating models, resulting in efficiencies, convenience, cost savings and improved outcomes. While ICT is a key enabler, it is business requirements that will drive its use.

The benefits can accrue not only to Municipality and Councillors but, through advances in digital technology, to the public in accessing and participating in Council and the IDP processes.

ICT will also reduce the impact on the environment through a reduction of paper and the need for travel. In the delivery of the ICT Master Plan, there will inevitably be a need to balance the requirement for flexibility of access with the need to keep Municipality and Councillors' data secure within budget constraints.

U.R.

4.7 ICT Strategic Imperatives

The ICT Master Plan is defined through strategic imperatives that outline the key areas where PKSDM ICT will focus planning, investment and delivery of ICT services to connect Council Members, the public and the Council Service to the information and services they need from anywhere, at any time, through a range of devices, and provide new opportunities for greater efficiency and effectiveness for the District. This can be achieved by:

1. Supporting Council Members to be more effective through better use of ICT anywhere and anytime on a range of devices.
2. Supporting the effective and efficient operation of Council and its committees.
3. Making it easier for the public to engage with Council Members and the District.
4. Making it easier for the public to access services.
5. Transforming the ICT Unit into a capable, respected and forward looking ICT provider.

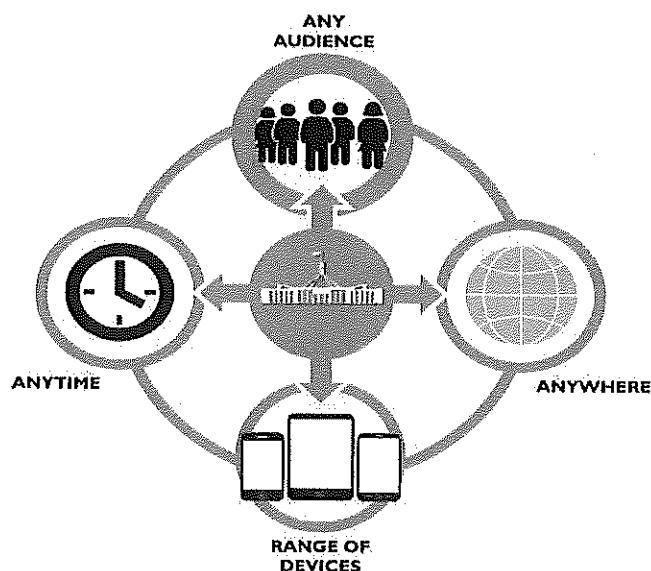


Figure 1: Information Ecosystem

The strategic imperatives will be supported by an underpinning architecture that enables content to be communicated and shared interactively with other individuals, teams and communities of interest.

Each strategic imperative includes a section outlining the key ICT capabilities required to deliver the specific business drivers. Some of these capabilities are common across multiple imperatives, but are only mentioned once, under the strategic goals that have the highest dependency to have it in place. The complete set of ICT capabilities will form the basis of the projects that will subsequently be planned to deliver the ICT Strategy.

4.8 Business view of ICT role

The PKSDM management and user community perceives the ICT unit to be reactive in terms of the role they play and rendering mainly technical and systems support services. However, they require that, in addition to rendering technical and systems support services, the ICT unit be more proactive and strategic and play a role in information management and information results management.

Another perception is that there are inadequate communication channels between the business and ICT and also lack of guidance on technology.

U.R.

4.9 Proposed ICT Structure

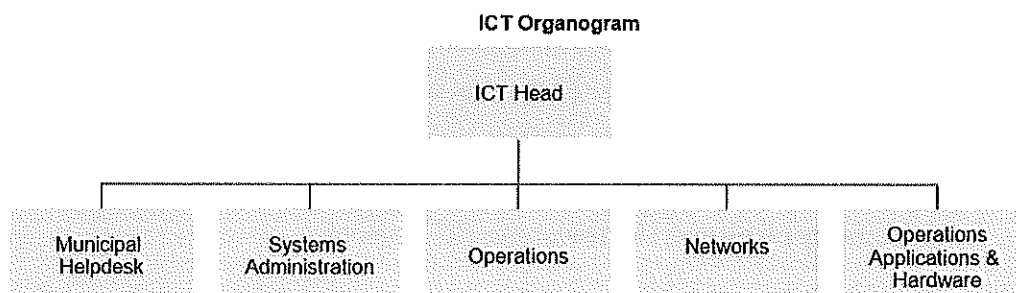


Figure 2: Ideal ICT Structure

PKSDM ICT has 2 people serving the municipality. The services rendered primarily include the following and this presupposes that the two are geniuses in everything offered under ICT, which is not the case:

Service	Description
Helpdesk	- Logging calls for faults with desktops, laptops, applications and systems; - Logging calls for Disaster Management; - Logging any other calls from citizens of the district
Operations	- Microsoft Word, Excel, PowerPoint and any other applications used within the municipality; - Hardware problem resolution; - Printing.
System Administration	- Operating software, legacy and vendor systems; - Password management; - Patch Management; - DRP & BCP Management.
Networks	- Connectivity (LAN/WAN WiFi); - Mobile connectivity; - Council chamber connectivity for virtual meetings; - e-Council.

There is need for 6 posts in total.

Proposed Organisational Chart: Office of the Municipal Manager

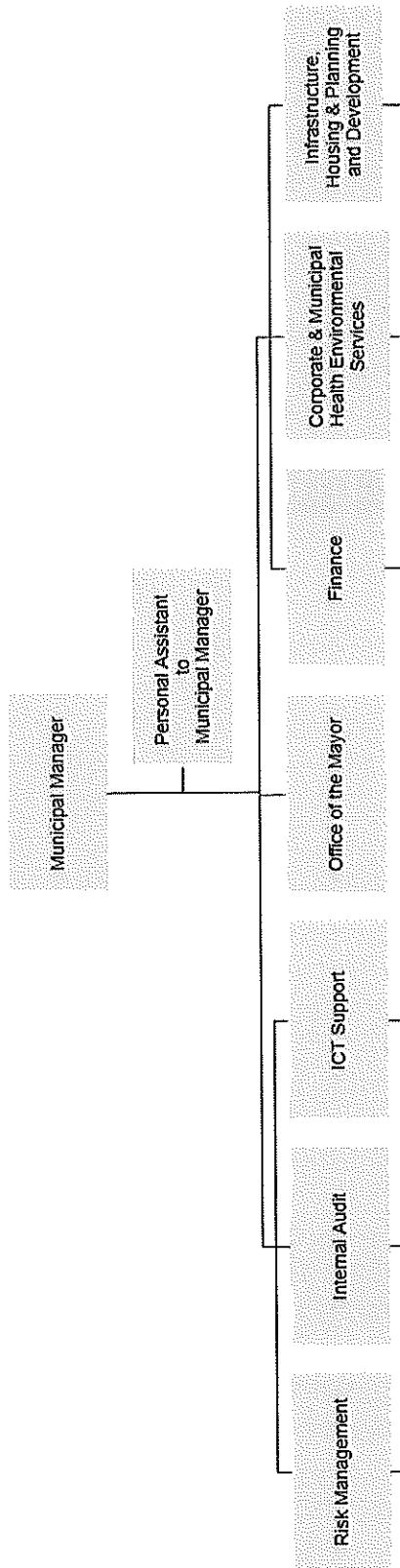


Figure 3: Proposed Structure - Office of the Municipal Manager

The current structure falls under corporate services and at a very junior level. This is not ideal especially now that we have entered the 4IR. This structure ensures that ICT is placed in a strategic position. It does not matter what title the person running ICT is called, but the person must assume the responsibility for a Chief Information Officer (CIO) and have requisite ICT skills. This is a pillar that supports the whole municipality and particularly the office of the municipal manager in terms of providing this office with a dashboard of all activities/projects on the go in the municipality at the press of a button.

Conceptual Architecture (CA)

U.K.

The conceptual architecture contains sets of global principles relative to and consistent across each architecture area within the Enterprise Architecture (*Business Architecture - BA, Information Architecture - IA, Technical Architecture - TA, and Application - AA*).

The conceptual architecture is the first segment in developing the individual architectural areas; the global principles reflect the collective and common will of PKSDM as they apply to the architectural area. Principles are guiding statements of position that communicate fundamental elements, truths, rules, or qualities that must be exhibited by an enterprise.

The purpose of principles is to enable PKSDM to take an incremental and iterative approach to transitioning to formal modelling, while allowing it to influence decision making immediately and consistently. The Principles are used as evaluation criteria in the absence of detailed models that direct decision making more discretely and comprehensively.

The bases for many principles are best practices – they are approaches that have consistently been demonstrated by diverse organisations to achieve similar results. Therefore, the degree to which an organisation can establish principles across the architecture areas is dependent on its ability to identify and apply best practices in each area. For this reason, TA principles tend to be more common than those of BA, IA, and AA are. The figure 1 below gives some examples of principles:

U.R.

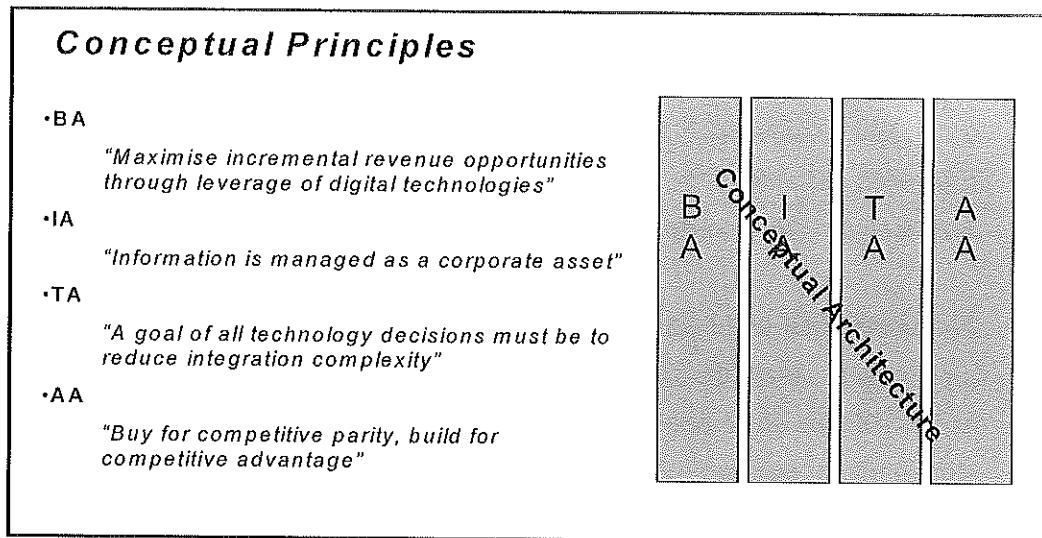


Figure 4: Conceptual Architecture

The conceptual architecture consists of Architectural Requirements, Best Practices and Principles. Each Best Practices (BP) contains Principles (PR). These components are described below.

5.1 Previous reading

It is assumed that the reader of this document has read and is familiar with the contents of the first components (which are Business Architecture and Common Requirements) of the Enterprise Architecture (EA).

5.2 Notation and Terminology

For reasons of consistency, the same notation as was used in the Business Vision and Common Requirements Vision will be used for identification and cross-reference purposes within this document (Conceptual Architecture):

- AR1 - Architectural Requirements
- BP1 - Best Practices
- PR1 - Principles

5.3 Architectural Requirements

Architectural requirements are high-level requirements, derived from business strategies and expressed as functional statements, which give direction and priority to each of the architecture areas comprising the Enterprise Architecture.

5.4 Best Practices and Trends

These are international best practices and trends relating to PKSDM as well as relevant information communication technologies.

5.5 Principles

Principles are guiding statements of position that communicate fundamental elements, truths, rules, or qualities that must be exhibited by an enterprise. They enable an organisation to take an incremental and iterative approach to transitioning to formal modelling, while allowing it to influence decision making immediately and consistently. They should be used as evaluation criteria in the absence of detailed models that direct decision making more discretely and comprehensively.

2. Conceptual Principles

The enterprise architecture's conceptual principles within PKSDM's computing environment include the followings:

2.1 Best Practises and Principles

The best practices identified in the EA Common Requirements Vision document have been added to and interpreted as principles. "Ownership" and "Applicability" for each principle is also indicated. "Ownership" implies that the architecture area is responsible for maintaining the principle as well as ensuring that any policies, procedures, standards and guidelines required for the support of the principle are developed. "Applicability" indicates which architecture areas the principle applies to.

5.5.1 BP1 Evolving a Holistic Enterprise Architecture

Organisations impacted by increasing rates and amount of change are faced with the challenge of modelling and analysing the impact of change across various parts of PKSDM. The relationships between business processes, information and applications are highly interdependent. This requires an adaptive integrated Technical Architecture (TA) to enable the leveraging of information communication technology.

5.5.1.1 PR1 Skilled Business Technologists

As ICT is increasingly becoming a key enabler of business, it is vital that individuals within the business have a thorough understanding of the business and the technologies that enable or can enable the business. This key role is termed the "business technologist".

(Owner: **BA** also applies to: **TA**)

5.5.1.2 PR2 Common Vision

ICT and the business must share a common vision to ensure that the strategic goals of the PKSDM are achieved. This is the combined role of the Business Vision and the Common Requirements Vision (CRV).

(Owner: **BA** also applies to: **IA, TA** and **AA**)

5.5.1.3 PR3 Single Corporate Planning Process

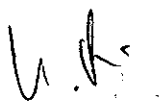
The business and ICT strategic planning processes should be integrated.

(Owner: **BA** also applies to: **IA, TA** and **AA**)

5.5.1.4 PR4 Visible Strategy

The Enterprise Architecture (including Business strategy) and its supporting structures must be communicated and made visible to all levels.

(Owner: **BA** also applies to: **IA, TA** and **AA**)



5.5.1.5 PR5 IT: Strategic Investment for Business Enablement

Historically ICT has been perceived as a cost to the business with no real benefit. Given the dependency of business on ICT to remain competitive, it must be seen as a strategic investment and a critical business enabler.

(Owner: **BA** also applies to: **IA, TA** and **AA**)

5.5.1.6 PR6 Enterprise Models

The enterprise architecture must model the business design, information, application and technology infrastructure. They are required to assess the impact of change and to identify gaps and opportunities. This requires business and ICT modelling methodologies and tools that conform to the Technical Architecture standards.

(Owner: **BA, IA, TA** and **AA**)

5.5.2 BP2 Reduce Integration Complexity

The old approach of vendor-based vertical solutions led to a diversity of vendors with incompatible information technologies. Best practice is to implement horizontal solutions which are highly compatible across the organisation. A goal of the enterprise architecture is to reduce integration complexity across all architectural domains.

5.5.2.1 PR7 Open Standards

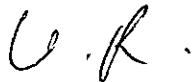
All technology and systems development must adhere to open system standards across all technical domains.

(Owner: **TA** Also applies to: **IA** and **AA**)

5.5.2.2 PR8 Process-Driven Business Solutions

Design process-driven solutions that cut across the organisation (as opposed to functional solutions which lead to duplication).

(Owner: **IA** also applies to: **BA, TA** and **AA**)



5.5.2.3 PR9 Technology Standards

All technology solutions must conform to appropriate international and national standards to enable integrated solutions and to facilitate the introduction of new technologies. This will require a governance process for the introduction of new standards or modifying existing standards.

(Owner: TA Also applies to: IA and AA)

5.5.2.4 PR10 Portability and Scalability

Application systems and databases must be platform independent, robust and scalable upwards or downwards.

(Owner: AA and TA)

5.5.3 BP3 Leverage IT

Competitive advantage can be attained through the innovative use of information technology within PKSDM computing environment.

5.5.3.1 PR11 Technology/Digital Innovation

The application of this principle requires that PKSDM:

- Evaluate the applicability of technologies to business needs via "Proof of Concept" exercises jointly with all relevant partners (including business);
- Maintain a budget(s) and resources for Research and Development purposes;
- Identify opportunities for digital innovation in business process design.
- Are "Followers" and not "Leaders". (Risk management procedures must be adhered to); and
- Use networking forums such as standards and research bodies, internet, etc.

(Owner: TA also applies to: BA and AA)



5.5.4 BP4 Information is valued as an enterprise asset

The value of information sharing and the potential commercial value thereof are not always recognized. It must be shared to maximize the effectiveness of business decision making throughout the PKSDM and beyond to external partners (extended value chains). Decision making must accelerate to increase the organisations' responsiveness to rapidly changing requirements. Information must also be managed to increase the integrity and relevance of data.

5.5.4.1 PR12 Data Management

Apply data management principles throughout the organisation. These are to include the following:

- Data isolation;
- Standard data access mechanisms;
- Controlled duplication and replication;
- Validated and corrected data at source;
- Data captured once only;
- Defined roles and responsibilities (e.g. ownership, stewardship, content management);
- Data naming standards;
- Data redundancy procedures;
- Data archiving procedures;
- Quality assurance of data; and
- External data handling procedures.

(Owner: **IA** also applies to: **TA** and **AA**)

5.5.4.2 PR13 Information Sharing

Information must be shared to maximise the effectiveness of business decision making throughout the enterprise and beyond to external partners.

(Owner: IA also applies to: BA, TA and AA)

PR14 Information Protection

Policies and procedures must be defined to address the following:

- Data access security;
- Information classification in terms of privacy, confidentiality, etc.;
- Backup and disaster recovery;
- Internal and external data access security;
- Virus protection; and
- Change management.

(Owner: IA also applies to: BA, TA and AA)

5.5.4.3 PR15 Metadata

Metadata (Metadata is the warehousing of all PKSDM data giving PKSDM views of this data which do not exist elsewhere) must be defined for all PKSDM corporate data and must be made accessible to the enterprise.

(Owner: IA also applies to: TA and AA)

5.5.5 BP5 Leverage BI and MIS

Reduced business cycle times have led to a need for accelerated decision making and more information access. There is a significant burden on users to generate reports and data queries. The business intelligence and MIS environments consisting of data warehousing and operational data stores, together with appropriate analytical tools, make it possible and easy to execute these tasks.



5.5.5.1 PR16 PKSDM Corporate Data Positioning Guidelines

Corporate data is positioned in one of the following three areas based on usage:

- Operational data;
- Management information; and
- Decision support.

Guidelines and design principles relating to the use of corporate data must be defined and adhered to.

(Owner: **IA** also applies to: **TA** and **AA**)

5.5.5.2 PR17 OLTP / OLAP Separation

OLTP (On-line Transaction Processing) relates to the processing of operational transactions where performance and throughput are critical.

OLAP (On-line Analytical Processing) relates to the searching and analysing of data, which have different processing demands.

Production data from applications should be loaded into the management information and business intelligence environments for user reporting and analysis using standard tools. This requires formal data extraction, propagation and replication procedures.

(Owner: **TA** also applies to: **IA** and **AA**)

5.5.6 BP6 Unified Architecture Management

Planning and management of the architecture must be unified, whether PKSDM decide to decentralise ICT responsibilities or not. This is to avoid diversity among priorities/trade-offs, principles, product standards, and configurations.

5.5.6.1 PR18 Architectural Governance

Appropriate governance structures and procedures are required to ensure a unified approach. The governance process must involve both the business and ICT.

(Owner: **BA** also applies to: **TA, IA and AA**)

5.5.7 BP7 Governed Evolution

The enterprise architecture must have a planned evolution that governs across PKSDM. Enterprise architecture is a process; it takes time and involves change. Good change requires collaboration and collective planning. Architecture must be well thought out and not established in a "hit or miss" fashion. Short term activities versus long term goals must be constantly examined requiring prioritisation and re-prioritisation across all ICT initiatives.

5.5.7.1 PR19 Architecture Planning and Implementation

All architectural initiatives must be planned, co-ordinated, funded and prioritised jointly according to the project management standards.

(Owner: **Corporate Services** (this is in accordance with the PKSDM organisational structure. also applies to: **BA, IA, TA and AA**)

5.5.7.2 PR20 Short-term Bridging Policy

A bridging policy is required to guide the deployment of short-term or interim solutions until such time as an ICT strategy exists.

(Owner: **TA** also applies to: **BA, IA and AA**)



5.5.8 BP8 Event-Driven

5.5.8.1 PR21 Event-Driven Systems

Deploy applications that are business event-driven so as to increase adaptive ness to changes within business processes which are a series of business events.

(Owner: **AA** also applies to: **TA**)

5.5.9 BP9 Application Re-engineering

Application systems development should enable and leverage re-usable components or application modules which are platform independent to achieve adaptability and flexibility.

5.5.9.1 PR22 Granulation and Coupling of Application Systems

Application systems should be re-engineered to become highly granular (ideally a maximum of one function per module) and loosely coupled (independent free-standing modules based on components which can be combined or separated using industry standard technologies).

(Owner: **TA** also applies to: **AA**)

5.5.10 BP10 Build for Competitive Advantage

The use of packaged solutions is increasing and will continue through 2008. Because the same packaged solutions are available to the competition they will not enable the business to sustain competitive advantage.

5.5.10.1 PR 23 “Build” or “Buy” Applications

Build or assemble from components applications that will provide competitive advantage and buy applications that will provide competitive parity.

Areas that provide competitive advantage are likely to be areas in which quick adaptation is required. This requires in-house, not vendor, responsibility.

Differentiation, not operational excellence is the competitive advantage for most market leaders.

Guidelines in terms of when to "buy" and when to "build" are required. (e.g. based on fit with specified criteria, etc.)

(Owner: **AA** also applies to: **TA**)

The following principles are additional to those identified in the CRV and are of a more technical nature:

5.5.11 BP11 Logical Partitioning

Partitioning isolates and minimises the impact of change whilst enabling adaptability and flexibility.

5.5.11.1 PR24 Logical Partitioning

The logical design of application systems should be highly-partitioned into discrete service layers, which include presentation, process, data request and data access.

(Owner: **TA** also applies to: **AA**)

5.5.12 BP12 Messaging

This allows for location, DBMS (database management systems) and data structure transparency and is a key enabler of a number of the best practices listed.

5.5.12.1 PR25 Message-Based Interfaces

The interfaces across separate logical boundaries must be message-based and extend across the value chain to both customers and suppliers.

(Owner: **TA** also applies to: **IA** and **AA**)



5.5.13 BP13 Enterprise Network as a Virtual LAN

An enterprise backbone network must be implemented which provides a “single network image” as if it were a virtual, enterprise-wide LAN (local area network).

Knowledge-workers have an increasing need for access to information across the enterprise and this access should be seamless to reduce decision-making cycle times. The lack of robust network architecture will impact the success of distributed applications as networks are the essential enabling technology for N-tier, Internet and collaborative computing.

5.5.13.1 PR26 Network Interface

The user must have a transparent, seamless and consistent interface with the network. This will require standard protocols.

(Owner: **TA** also applies to: **AA**)

5.5.14 BP14 Server Partitioning (“Workloads”)

Applications and databases should be physically partitioned on separate servers, in the same location, based on workload. Server configuration (processors, memory, storage, etc.) is largely based on the expected volume and type of work.

5.5.14.1 PR27 Physical Server Boundaries

Physical boundaries must be established between application servers and database servers.

(Owner: **TA** also applies to: **AA**)

5.5.15 BP15 Appropriate Geographic Partitioning

Where adequate network infrastructure exists, applications and databases should NOT be geographically partitioned. Network bandwidth and management tool maturity make this possible.



5.5.15.1 PR28 Server location

Applications and database servers must be located in a data centre, room, cloud storage and on the same network infrastructure.

(Owner: **TA** also applies to: **AA**)

5.5.16 BP16 Virtualisation

Geographic partitioning should be delivered using the concept of a virtual data centre. Servers in a virtual data centre are configured and maintained exactly like servers in a real data centre.

5.5.16.1 PR29 Virtual Data Centre

Geographically distributed data must be centrally managed according to the same standards and procedures.

(Owner: **TA** also applies to: **AA**)

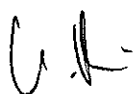
5.5.17 BP17 Architecture Ownership

Architecture development is internally owned and managed.

5.5.17.1 PR30 Architecture In-Sourcing

Enterprise architecture is a strategic enabler and development therefore must be an in sourced effort and never be outsourced. Architecture comprises principles based on that enterprise's business needs, and it is used to guide the internal engineering efforts within the enterprise. These guiding principles cannot be impacted by the incentives and motivations that external partners invariably have. Architecture development skills are expensive, so a continual return on investment is desired.

(Owner: **BA** also applies to: **IA**, **TA** and **AA**)



5.5.18 BP18 Application Programming

Whether application is developed in-house or outsourced, it must align with the architecture standards and principles.

5.5.18.1 PR31 Define Programmer Domain

A sustainable and scalable method of rapid application development is needed to respond to collapsing business cycle time.

To achieve "Enterprise RAD", PKSDM must redefine the application domain to align with the business rapidly changing needs.

(Owner: **TA** also applies to: **AA**)

5.5.19 BP19 Infrastructure Re-use Development

Infrastructure development is a separate team and a core competency to deliver reusable infrastructure services to business applications. Reuse requires a focus. TA guides ICT toward reusable components of infrastructure and provides standard application interface services to infrastructure within PKSDM computing.

Employ infrastructure pattern matching in infrastructure design.

Infrastructure development must provide application interface services to access reusable infrastructure components.

Applications' technical designs must conform to the use of infrastructure development for interface services.

5.5.19.1 PR32 Infrastructure Patterns

Employ the concept of infrastructure patterns for infrastructure design. Infrastructure patterns are re-usable design patterns, frameworks and methodologies.



(Owner: **TA** also applies to: **AA**)

5.5.20 BP20 Value Add

Business value sourcing will replace traditional return-on-investment and total-cost-of-ownership measures as the primary metric for measuring the success of the enterprise architecture.

5.5.20.1 PR33 Value Measurement

Measurement of the contribution of EA to the achievement of business objectives can be achieved by for e.g.:

- Conducting maturity audits at regular intervals;
- Conducting quality assurance assessments (ISO 9001);
- Obtaining user satisfaction ratings;
- Maintaining metrics on responses to business needs (time, cost); and
- Monitoring system availability.

(Owner: **BA** also applies to: **IA**, **TA** and **AA**)

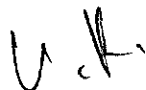
5.5.21 BP21 Rapid Decision-Making

Rapid decision-making requires real-time access to data.

5.5.21.1 PR34 real-time access to data

Systems should move from batch orientation to on-line real-time where appropriate.

(Owner: **AA** also applies to: **TA**)



5.6 Matrix of Best Practises and Principles

The following matrix cross-references the principles as they apply to the individual architecture areas. "O" = Owner, "A" = Applicable.

Principle	Description	BA	IA	TA	AA
PR1	Skilled business technologists	O		A	
PR2	Common Vision	O	A	A	A
PR3	Single Corporate Planning process	O	A	A	A
PR4	Visible Strategy	O	A	A	A
PR5	IT: Strategic investment and a Business enabler	O	A	A	A
PR6	Enterprise Models	O	O	O	O
PR7	Open standards		A	O	A
PR8	Process-driven business solutions		O	A	A
PR9	Technology standards		A	O	A
PR10	Portability and scalability			A	O
PR11	Technology/Digital innovation	A		O	A
PR12	Data Management		O	A	A
PR13	Information Sharing	A	O	A	A
PR14	Information Protection	A	O	A	A
PR15	Metadata		O	A	A
PR16	Corporate Data Positioning Guidelines		O	A	A
PR17	OLTP / OLAP separation		A	O	A
PR18	Architectural governance	A	A	O	A
PR19	Architecture planning and implementation	A	A	A	A
PR20	Short-term bridging policy	A	A	O	A
PR21	Event-driven systems			A	O
PR22	"Highly granular" and "Loosely coupled" application systems			A	O
PR23	"Build" or "Buy" applications			A	O
PR24	Logical Partitioning			A	O
PR25	Message-based interfaces		A	O	A

U-R

Principle	Description	BA	IA	TA	AA
PR26	Network interface			O	A
PR27	Physical server boundaries			O	A
PR28	Server location			O	A
PR29	Virtual Data Centre			O	A
PR30	Architecture in Sourcing	O	A	A	A
PR31	Redefine Programmer Domain			O	A
PR32	Infrastructure patterns			O	A
PR33	Value Measurement	O	A	A	A
PR34	Rapid decision-making requires real-time access to data			A	O

Figure 5: Principles Matrix

U. H.

Business Architecture (BA)

U.R.

6 Management Summary

The initial focus was to get the "big picture". Techniques applied in getting the big picture were Enterprise Value Network (EVN) modelling and Information Value Network (IVN) modelling as well as business scenario modelling. Details on these techniques are in the latter part (section 4.1) of this document. The goal is to model just enough of the business functions, processes, and information flows to facilitate decision making, perform impact analysis, identify digital innovation opportunities, and create a macro view of the Enterprise Architecture (EA) future-state for PKSDM.

After the big picture was established, the Business Architecture (BA) selectively drilled down into key processes using business event modelling, zone modelling, integration modelling, and function/process decomposition models for those parts of the business impacted most by changing business strategy.

The business architecture is dependent on the:

- Business Vision (BV) which provides a clear vision of "business futures" by capturing the most important enterprise business strategies being pursued at the time;
- Common Requirements Vision (CRV), which consists of high level architectural requirements (*derived from the business strategies in the BV and expressed as functional statements*). These give direction and priority to each of the architecture disciplines comprising the Enterprise Architecture (i.e. BA, IA, AA, and TA).

The BA must evolve as a joint venture between the strategic planners (executive and managers) and process innovators (this includes all employees) within PKSDM, which includes all business units and the ICT department. The charter of the BA evolution defines the business processes, digital technologies, and information that can be leveraged to maximise value for PKSDM.



The BA component of the EA expresses the PKSDM's key business strategies/tactics and their impact or interaction with business functions and processes that:

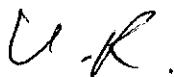
- Typically consist of the current- and future-state models of business functions, processes, and information value chains;
- Lead to the development of the Information Architecture (IA), the Application (AA) and Technical Architecture (TA); and
- Define the business design for sustainable competitive advantage.

7.1 Purpose

The objective of the BA is to define what high-velocity information must pass between what key processes, and the integration requirements that must be enabled by the underlying application architecture and technical architecture.

While the BA is not required to create an adaptive TA, it is a prerequisite for developing the enterprise architecture (EA) and enables decision makers to:

- Explore digital innovation opportunities;
- Integrate business and IT strategy development;
- Analyse impact, risk and "what-if" scenarios;
- Optimise value chains;
- Value IT investments via information value;
- Design innovative business processes;
- Analyse application requirements;
- Plan application portfolios;
- Increase velocity of information across the enterprise (*further dealt with in the IA*); and
- Evolve the Enterprise Architecture (EA).



7.2 Evolution Approach

The BA must evolve as a joint venture between the strategic planners (executives) and process innovators (all employees) within the ICT organisation. Strategic planners within corporate and business unit management provide input on business strategies. The business units focus on the definition of process innovation opportunities and the ICT Systems Administrator (EA sponsor) focuses on the definition of digital innovation opportunities. The charter of the BA evolution defines the business processes, digital technologies, and information that are leveraged to maximise value for PKSDM.

The initial focus for developing the BA was to get the "big picture", as drilling down into a detailed analysis of business processes, events and information flows would have been wasted effort if the scope of the BA was not defined. Various modelling techniques were applied to get the big picture. The goal is to apply "just enough modelling, just in time", and with this point in mind, after the big picture is established, the BA design then selectively drills down into key processes using various modelling techniques to establish business patterns.

7.3 Previous Reading

It is assumed that the reader of this document has read and is familiar with the contents of the Business Architecture, Common Requirements Vision, and Conceptual Architecture documents of the Enterprise Architecture for PKSDM.

7.4 Notation and Terminology

The following notation will be used for identification and cross-reference purposes throughout this document:

AR1	through Arxx	-	A rchitectural R equirements
BR1	through BRxx	-	B usiness Architecture R equirements
PR1	through Prxx	-	P Rinciples
P1	through Pxx	-	C ore P rocesses



1. Architectural Requirements (AR)

The architectural requirements are high-level requirements, derived from the PKSDM IDP and expressed as functional statements, which give direction and priority to each of the architecture disciplines comprising the Enterprise Architecture (*i.e. business architecture, information architecture, application architecture and technical architecture*).

2. Business Architecture Requirements (BR)

The business architecture (BA) requirements are architectural requirements pertaining to the business architecture.

3. Principles (PR)

Within the EA, Principles are guiding statements of position that communicate fundamental elements, truths, rules, or qualities that must be exhibited by an enterprise. The principles will enable PKSDM to take an incremental and iterative approach to transitioning to formal modelling, while allowing it to influence decision making immediately and consistently. The principles should be used as evaluation criteria in the absence of detailed models that direct decision making more discretely and comprehensively.

4. Core Processes (P)

The core processes are the high-level processes performed by each core business within PKSDM.

5. Best Practices and trends (BP)

The best practices and trends are international best practices and trends relating to zone and property development and management as well as to relevant technologies.

C. R.

8 Drivers for Business Architecture

8.1 Architectural requirements for Business Architecture

The following requirements for business architecture have been derived from the overall architectural requirements (AR1 to AR7) as identified in the Common Requirements Vision (CRV) developed for the PKSDM.

AR1 Implement strategies with minimal impact on service delivery.

BR1 Enable the rationalisation of core business processes across the organisation;

BR2 Ensure that the PKSDM organisational roles and responsibilities are defined;

BR3 Enable effective transition planning and co-ordination;

AR2 Compete in a global economy according to best practices and trends.

BR4 Enable the streamlining and automation of core business processes across functions;

BR5 Ensure that a Human Resource planning process is accommodated;

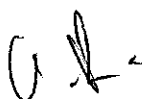
BR6 Ensure that a business Research and Development function is accommodated;

AR3 Deliver flexibly packaged and priced services

BR7 Enable the definition, analysis and segmentation of the customer base

BR8 Ensure the provision of adequate and appropriate service delivery mechanisms

BR9 Enable differentiated service pricing mechanisms where appropriate and required



AR4 Monitor, measure and track service delivery to clients

BR10 Ensure the identification and currency of benchmark standards;

BR11 Ensure appropriate control mechanisms are identified and implemented;

AR5 Provide controlled access to reliable and secure information

BR12 Ensure appropriate information management policies are implemented.

AR6 Cost Effectiveness

BR13 Enterprise architecture development and implementation must be cost-effective.

AR7 Enable good governance according to best practices and trends

BR14 Ensure the implementation of performance measurement and evaluation mechanisms for management and public (partners, stakeholders, shareholders and clients) representatives.

8.2 Business Processes

As defined in the EA Business Vision, PKSDM is dependent on the following business processes for the successful operation and management of the business.

8.2.1 Core Processes

The following core processes have been identified:

P1 Supply and maintain municipal services;

P2 Conduct and promote planning and development;

P3 Identification and local economic development;

P4 Manage and maintain land and infrastructure; and

P5 Conduct disaster management.

8.2.2 Support Processes

The following support processes are required in support of the core processes:

- P6** Administration;
- P7** Finance;
- P8** Information and Communication Technology;
- P9** Human Resources;
- P10** Project Management; and
- P11** Logistics.

8.3 Conceptual Principles

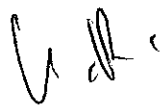
Conceptual principles have been extracted from the Conceptual Architecture as they pertain to the BA and are further broken down into business principles, standards and guidelines.

9 Business Architecture Deliverables

The Business architecture deliverables includes the architectural principles (section 3 above), gap analysis (appendix A), business architecture set of checklist (appendix B) and business models framework (section 4.1 below).

9.1 Business Models

The PKSDM BA is designed to model just enough of the business functions, processes and information flows (which constitute business patterns) to facilitate decision making, perform impact analysis, identify digital innovation opportunities and create a macro view of the future state adaptive Enterprise Architecture. The enterprise models evolve over time according to priority and need.



The BA's design selected key processes and modelled them further using techniques such as business event modelling, zone modelling, and integration modelling and functional/process decomposition. Details of the various models are provided in the latter part of this section. Figure 1 below depicts the overall framework for performing the BA modelling and as well as details the linkages of BA to the other components of the overall EA.

9.1.1 "The Big Picture" (Enterprise Value Network)

The techniques as depicted in figure 1 below, which serve as framework, provide PKSDM business leadership with a "big picture" of the enterprise, stimulates an interactive dialogue for evolving the overall BA, and to implement a blue-print for enterprise business design:

- enterprise value network modelling;
- information value network modelling; and
- business scenario modelling.

9.1.2 Enterprise Value Network (EVN)

According to Michael Porter ("Competitive Advantage", Michael Porter, 1985), the value chain, has exploded into the Enterprise Value Network in most organisations in view of the availability of information and the emerging ability to electronic business.

Business Architecture modelling at the "big picture" level is a creative exercise and brainstorming techniques using a white board or flip chart, are appropriate tools for the first round of high-level BA definition. This exercise was conducted with the management team on one-on-one and in groups where time permitted.

Value networks define the critical functions required to deliver products, both internal and external, and the relationships in place to provide those functions. The new business environment resembles a web of fluid, ever-changing



relationships -nodes on a network - rather than a fixed distribution channel. See figure 2 below.

The ICT System Administrator needs to dissect the current business chain, catalyse the construction of a new one, and then build the adaptive infrastructure (business functions, organisation structure, roles, and technology) to support all business value opportunities. This effort will be assisted by asking questions such as:

- i. Where within the value chain is information a key component of value?
- ii. Where are there opportunities (or risks) for critical portions of the value chain to be peeled off as a standalone business?

The first step in analysing the value network is understanding of the business strategy, vision and goals (as articulated in the Business Vision, Common Requirements Vision and Conceptual Architecture documents) that become the primary input to the EVN definition (*refer to Figure 6 below*). The key goal in exploring the business value network must determine:

- Are activities supporting PKSDM corporate goals?
- Is the activity performed by the organisation a core competency, or is there an opportunity to increase value by partnering?
- If a partnership is in place, what is the value of the partnership, and how does the relationship support the organisation's competitive strategy?

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
▪ Overall PKSDM business context ▪ Business "ecosystem" ▪ High- level representation of the externalised enterprise ▪ Value of key activities and partners	▪ Alliance partners ▪ Key activities ▪ Value of the alliance ▪ Primary sources of value ▪ Strategic alignment	▪ Who are PKSDM key alliance partners? ▪ What key functions and processes are involved? ▪ What is the value of the alliance? ▪ What is the source of value (competitive strategy): ▪ Operational excellence, customer intimacy, or	▪ Common requirements vision ▪ ICT (IA & AA) ▪ Business patterns ▪ IVN models

		product leadership? ■ Is the value of the partnership aligned with competitive strategy?	
--	--	---	--

Figure 6: Enterprise Value Networks Definition

Combination of graphical models and descriptive text must be adopted in the documentation of the modelling artefacts at all times. A value network model should be created that depicts the vertically and horizontally linked business structure with descriptive text as appropriate. Spreadsheets may be used to describe and rank the alliance partner information and key functions.

9.1.3 Information Value Network

The Information Value Network (IVN) model describes the linkages in the value network and the value of the information product across the value network. Linkages exist horizontally between business units and vertically between suppliers, partners, and customers. Information is an artefact of business processes - it surrounds and supports the physical value chain. The value of information (*Infonomics*) is determined by the "competitive advantage" gained by the use of the information product. It is the price premium that the consumer of information is willing to pay that exceeds the extra cost of providing the information product. There are essentially three dimensions of information value (*velocity, density and reach*) and the value of information can be increased by moving along one or more of these dimensions.

Information value network analysis is used to diagnose problems or uncover opportunities to leverage information technology to create high value, low cost linkages with external parties and across the lines of business (LOB). Each of the nodes in the IVN is analysed to determine:

- What are the key information products within the vertically and horizontally linked business structures?;

U. R.

- What are the characteristics of the linkage - density, velocity, cost and value?; and
- What opportunities are there to leverage information products to decrease costs, increase value, or increase velocity?

Figure 7 below describes the approach to IVN modelling. The documentation of the modelling artefacts should include a combination of graphical models and descriptive text. Models should depict the key information stores and flows between major business functions along the EVN.

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
▪ Overall IVN logistics ▪ Define high velocity information (HVI) requirements ▪ Define key externalisation opportunities ▪ Define key information product leverage points	▪ Key IVN processes ▪ Key IVN information flows ▪ HVI requirements	▪ What key information products can be leveraged to improve decision making?	▪ Common requirements vision ▪ TA domain architectures ▪ IA

Figure 7: Information Value Network Definition

Digital innovation opportunities should be indicated as appropriate and descriptive text should be used to describe the key elements of the IVN.

9.2 Business Scenarios

The business scenario modelling pulls the artefacts of the EVN and IVN models into a series of alternative future-state business designs. Business scenarios are used to communicate the digital innovation opportunities to executive and management in such a manner that they can rank the alternatives and select the appropriate course of action.

Figure 8 below summarises the approach to business scenario modelling. The modelling artefacts should be documented using a combination of graphical models and descriptive text to describe the PKSDM business scenario. Spreadsheets may be used for ranking and prioritising alternatives.

G H

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
▪ Visioning ▪ Refine business strategies ▪ Test strategy assumptions ▪ What-if analysis of alternative business architectures ▪ Select/rank business architecture alternatives ▪ Demonstrate value of digital innovation opportunities	▪ Business scenarios ▪ Digital innovation scenarios ▪ Ranking of alternatives	▪ What are the possible business scenarios to respond to an environment trend/business driver? ▪ How can digital technology be used to create innovative business architectures?	▪ Common requirements vision ▪ AA ▪ IA

Figure 8: Business Scenario

9.3 Business Patterns

After the "big picture" is established, the business architecture selectively drills down into key processes, business events, and information flows to discover new opportunities for innovation, while modelling new business patterns to be followed by the enterprise. This is accomplished by creating a series of models that further detail the high-level BA using:

- business event analysis;
- function/process decomposition; and
- integration modelling.

Business patterns are used to describe and model the new enterprise, communicating the desires of management while providing a foundation for organisational and technological designs.

A business pattern is a collection of artefacts used to describe the new processes at the time, functions, information flows, and organisational changes required by the high-level BA value relationships.

By documenting the new business patterns of the organisation, the BA team is providing critical information for the future architecture. The implications of the new business patterns are changes to:

G. R.

- The relationship and functionality of applications in the application architecture;
- The infrastructure required and guided by the technical architecture; and
- The velocity of information for the information architecture.

Figure 8 above details the linkages of the BA to the other components of the overall enterprise architecture.

Documenting business patterns is part art and part science. Business patterns provide further visualisation of the roadblocks to digital innovation and the analysis and modelling thereof should be viewed as a creative effort.

Several formal modelling tools can be helpful in the creation of more technical models, however, standard graphic, word processing and spreadsheet tools will suffice for the models described thus far.

9.4 Business Event/Process Model

The business event/process model is accomplished by selecting the business event (e.g. customer requests such as municipal services) to pattern, documenting the current means of handling the event, and evaluating options for improvement. It is the business event *design* artefact of the BA.

The business event/process model should:

- utilise a cross-functional team for the discussion;
- set the scope of analysis to answer the critical question posed during review of the high-level BA;
- identify the initiator of the business event; and
- document the most crucial artefacts created and used during the processing of the event.

Further exploration of the connections between the highlighted nodes of the value network model reveals the means to improve operational efficiency and



gain competitive advantage through reductions in event-processing cycle time.

Figure 9 below provides guidance for the event/process modelling.

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
▪ Enable selective understanding of key business events along the EVN ▪ Analyse opportunities to optimise business processes ▪ Enhance operational effectiveness, customer intimacy, product leadership ▪ Evolve the IA, AA and TA	▪ Major business event participants ▪ Alliance partners ▪ Identification of crucial process artefacts ▪ Validation of innovation ▪ New business pattern	▪ Who is the initiator of the business event? ▪ How does the event flow through the virtual enterprise?	▪ IA ▪ function/process decomposition ▪ AA ▪ TA ▪ IVN models

Figure 9: Business Event/Process

9.5 Function/Process Decomposition

Function/process decomposition identifies the sub-processes performed by a business function, defines the scope of the major organisational entities, and captures the contribution of each business function participating in the value network.

Function/process decomposition **should**:

- Set the scope of the analysis to the crucial business functions participating in the value network;
- Identify the major processes performed by a business function;
- Identify cross-functional processes - opportunities for digital innovation;
- Identify overlaps and redundancies; and
- Function/process decomposition **should not**:

- a. Document every business function in the organisation; and
- b. Involve descriptions of more than one or two pages.

In addition to the above, figure 10 below is critical in the decomposition of PKSDM functions and processes.

U. R. J.

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
▪ Define the scope of each business function participating in the EVN ▪ Understand the sub-processes of each business function ▪ Provide a foundation linking the IA, AAP, and TA to key business functions	▪ Sub-processes of the major business functions ▪ Identification of redundant or low value-adding activities ▪ Application and information requirements	▪ What major functions are performed? ▪ What functions do not add value? ▪ What functions overlap with other business functions?	▪ IA ▪ Business event/process models ▪ Location models ▪ AA

Figure 10: Function/Process Decomposition

9.6 Geographic Model

Geographic model identifies where a business function is performed and represents a logistical view of PKSDM business functions involved in the value network. The goal of zone modelling is to visualise the organisational structure as a function of the current and future EVN. It has the added benefit in that it identifies the architecture requirements imposed on the technical architecture by zone-to-zone interaction.

Geographic models should:

- focus on the business functions participating in the value network;
- show the locations performing the function;
- show linkages between entities in the EVN;
- Location models should not;
- Be a network diagram; and
- show all possible connections on the same diagram.

Figure 11 below contains primary criteria for zone modelling within PKSDM enterprise.

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
▪ Understand where the functions and processes are	▪ Function by business zone ▪ Linkages between business functions	▪ Where are major functions performed?	▪ Business event/process models ▪ TA

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
- actually implemented - Understand the implications of geography on BA and TA decisions - Understand the TA requirements for geographic distribution	- TA and application portfolio requirements - Opportunities for organisational change	- What functions are linked together? - Do consolidation and streamlining opportunities exist?	AA

Figure 11: Zone Modelling

9.7 Integration Modelling

An integration model shows the high-level interface requirements to process a business event, and it documents the information requirements of the new business pattern as well as the timeliness requirements. It serves as a starting place for the information architecture and application architecture, while providing input for the technical architecture regarding business information and architecture requirements for integration services.

Integration models should:

- Focus on the business events modelled for the new business pattern;
- show the information flowing between event participants; and
- focus on the critical information requirements.

Integration models should not:

- be the enterprise information architecture;
- be a data model;

In achieving the aim of the integration modelling, figure 12 below should be applied as the guiding principles as well as incorporating the information flowing between the event participants.

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
- Understand the key integration points internal and external to the enterprise - Understand the key interfaces for applications	- Information flows required for the business pattern - Linkages between business functions - IA, TA, and AA requirements	- What information is critical to the new business pattern? - What flows between connections in the business event model?	- Business event/process models - IA - TA - AA

U. R.

Focus of Analysis	Artefacts of Analysis	Key Questions	EA Interface
Understand the TA requirements for integration	Opportunities for organisational change	What is the timeliness requirement?	

Figure 12: Integration Modelling

9.8 Organisation Architecture

The organisation architecture is a fundamental component of the business architecture and is required to ensure the smooth operation of the business. The main components of this architecture are:

1. An appropriate governance framework;
2. The roles and responsibilities required to support the identified key business processes; and
3. An appropriate organisation structure.

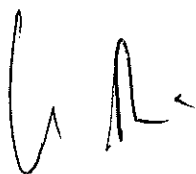
Information Architecture (IA)



The Information Architecture (IA) is the “information supply chain” extension of the PKSDM Business Architecture (BA). It is a business-strategy-driven set of artefacts that describe and model the PKSDM’s information value chain (*information flows, business events, linkages*). It extends beyond organisational boundaries to external sources and targets to enable rapid business decision making and information sharing. It also includes:

1. a catalogue of authentic sources of information (*e.g. government databases, commercial databases, research companies, and news media*);
2. classes of relevant business information and their value to PKSDM
3. information governance processes to support policy development and information management principles and practices that address: security access, privacy, confidentiality, information quality, integrity, authenticity, archival cycles, business resumption planning, and ownership; and
4. information management deliverables that address roles, responsibilities and organisation structure for managing information content and delivery (*e.g. information architecture group, custodian/steward, owner, chief knowledge officer*).

Development of the IA establishes the value and importance of using information effectively across lines of business within PKSDM, as well as the need to achieve collaborative excellence with external partners and customers.



11.1 Purpose

The Information Architecture (IA) is the “information supply chain” extension of the Business Architecture (BA). In keeping with the EA process principle of developing “just enough, just in time”, as with the BA, a **fully developed** IA is not required to create an adaptive Technical Architecture (TA). Instead it encourages decision makers to:

- Explore externalisation;
- Optimise information value chains;
- Plan application architecture and portfolios;
- Increase velocity of information across PKSDM; and
- Evolve the Enterprise Architecture.

The IA is a business-strategy-driven set of artefacts that describe and model the PKSDM's information value chain (*information flows, business events, linkages*) and is sponsored and endorsed by executive management and the lines of business. It extends beyond PKSDM organisational boundaries to external sources and targets to enable rapid business decision making and information sharing. It also includes:

- a catalogue of authentic sources of information (*e.g. company databases, commercial databases, research companies, and news media*);
- classes of relevant business information and their value to the enterprise
- information governance processes to support policy development and information management principles and practices that address: security access, privacy, confidentiality, information quality, integrity, authenticity, archival cycles, business resumption planning, and ownership; and
- information management deliverables that address roles, responsibilities and organisation structure for managing information content and delivery

U.R.

(e.g. *information architecture group, custodian/steward, owner, chief knowledge officer*).

Development of the IA establishes the value and importance of using information effectively across PKSDM lines of business, as well as the need to achieve collaborative excellence with external partners and customers. It is used to gain consensus between PKSDM management on:

- What is strategic versus non-strategic information
- The use and definition of common terms (e.g. service, consumption, customer, etc.)
- Who has the information, in what form, who owns/manages it, how it should be leveraged
- Who will be responsible for the cost of developing IT systems that will create and deliver information
- What metrics will be used to measure information sharing success (e.g. revenue increase, cost decrease, reduced service delivery times, etc.)

11.2 Notation and Terminology

The following notation will be used for identification and cross-reference purposes throughout the document:

AR1 - Architectural Requirements

I1 - Information needs

IR1 - Information Architecture Requirements

IP1 - Information Principles

1. Architectural Requirements

The architectural requirements are high-level requirements, derived from business strategies and expressed as functional statements, which give direction and priority to each of the architecture disciplines comprising the Enterprise Architecture (*i.e. business architecture, information architecture, application and technical architecture*).

2. Information Needs

PKSDM information needs reflect the information, regardless of source, required to facilitate strategic decision making as well as the successful management of the organisation.

3. Information Architecture Requirements

The information architectural requirements are derived from architectural requirements as they relate to the Information Architecture.

4. Information Principles

These are derived from global principles which are contained in the Conceptual Architecture.

12 Drivers for Information Architecture

The drivers for the information architecture consist of the architectural requirements and information needs as dictated by the PKSDM.

12.1 Architectural Requirements for Information Architecture

The following requirements for information architecture (IR1 to IR18) have been derived from the overall architectural requirements (AR1 to AR7) as identified in the Common Requirements Vision (CRV) for PKSDM.

AR1 Implementing Strategies

IR1 Eradicate uncontrolled data duplication and redundancy.

IR2 Introduce standards, controls and procedures, that will ensure the accuracy and integrity of information.

IR3 Catalogue / define and document corporate information sources (internal and external).



IR4 Classify corporate information sources according to specified criteria
e.g. function (*operational, management, strategic*), security
(*confidentiality, privacy, etc.*), time (*immediate, monthly, etc.*).

AR2 Workflows

IR5 Ensure that users can trigger workflow processes from one business unit
to the other;

IR6 Ensure that all documents created have version control;

IR7 Ensure that standard response times are triggered;

IR8 Ensure standardised data access and delivery mechanisms are
implemented across all platforms.

IR9 Ensure that information is integrated across common business subjects
(e.g. Customer).

IR10 Ensure that management information is readily available and accessible
through a controlled MIS environment.

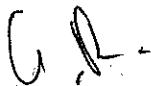
AR3 Flexibly Packaged Services

IR11 Ensure that MIS Incorporates GIS.

IR12 Ensure that the data architecture is structured to enable flexibility

AR4 Monitoring, Measuring and Tracking

IR13 Ensure that service delivery management information is readily available
through a controlled MIS environment.



AR5 Controlled Access

IR14 Enable the provision of access to information and data according to differing requirements in a managed and controlled environment.

There are three main areas involved in the processing of information. These are:

1. Business Operations - concerned with the operational (transactional) processing within PKSDM.
2. Business Management - concerned with measurement (keeping score) and management of the PKSDM, and
3. Business Intelligence - planning for the future and identifying competitive opportunities.

There are also different audiences requiring the information, both internally and externally. The architecture ensures that dissemination of information is controlled with appropriate access security in place.

The information may be sourced internally or externally, and it may be required on a corporate-wide basis or at a departmental level only. The architecture must ensure that all corporate information is defined and its sources catalogued.

AR6 Cost Effectiveness

IR15 Enterprise Architecture Development

Cost containment is a major factor in most of the business drivers. The development of the architecture must strike a balance between short-term goals and the sustained investment and change required to achieve the long-term vision.

AR7 Good Governance

- IR16** Ensure controlled access to information by the general public, which include stakeholders, clients and potential clients through appropriate media and channels.
- IR17** Ensure that management and external (investors, stakeholders, clients and potential clients) representatives have controlled access to information required for effective and rapid decision-making.
- IR18** Enable the performance management function, which must include measurement and evaluation within a controlled MIS environment.

12.2 Information Needs

As defined in the EA Business Vision, the PKSDM is dependent on the following information areas for the successful operation, the management of the business and for strategic decision-making:

12.2.1 Customer

The term “customer” relates to all who make use of the PKSDM’s services and facilities, including potential customers e.g. citizens, communities, businesses, investors, visitors, world-bodies, institutions, etc.

Information required about the customer includes:

- Nature of business;
- Location of business; and
- Contact details.

12.2.2 Geographical information

- Planning information;



- Survey information (topographical maps, aerial maps, survey grids, etc.); and
- Service layers (zones, road maps, etc.).

12.2.3 Assets/Property

- Ownership management;
- Valuations (market and municipal);
- Rates;
- Zoning; and
- Plans (building and development).

12.2.4 Human Resources

- Skills;
- Training;
- Remuneration; and
- Benefits.

12.2.5 Finance

- Income;
- Expenditure (operating and capital);
- Debtors (service consumers, rentals, leases, sundry debtors, etc.);
- Creditors (suppliers, service providers, contractors, etc.);
- Assets (current and fixed);
- Liabilities;
- Insurance; and
- Tax.

12.2.6 Governance

- Policies;
- Procedures;
- Standards;

G.R.

- Organisation (structure, roles, responsibilities - administrative) ;
- PKSDM by-laws, ordinances, etc.; and
- Contracts and agreements.

12.2.7 Services

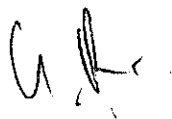
- Municipal services;
- Transport and logistics;
- Security engineering;
- Spatial Development;
- Land and infrastructure management;
- Disaster Management; and
- District Development Model Implementation.

12.2.8 External information

- Similar entities;
- Benchmarks; and
- Funding.

12.2.9 Conceptual Principles

Conceptual principles will be extracted from the Conceptual Architecture as they pertain to the IA and will be further broken down into information principles, standards and guidelines.



13 Information Architecture Deliverables

The Information Architecture deliverables includes the architectural principles (section 11 above), gap analysis (appendix C), and information architecture set of checklist (appendix D), business models framework (section 12.1 below), information management.

13.1 Information Management and Controls

The management and control of information requires:

1. **Information Governance processes** to support policy development and information;
2. **Management principles and practices** that address: security access, privacy, confidentiality, information quality, integrity, authenticity, archival cycles, business resumption planning, and ownership; and
3. **Information Management deliverables** that address roles, responsibilities and organisational structure for managing information content and delivery (e.g. information architecture group, custodian/steward, owner).

13.2 Information Sources

A catalogue of authentic information sources, such as company databases, commercial databases, research companies, and news media and so on, is used to establish the origins of authentic information on and about the organisation. It also forms the basis of input for the next step, which is to obtain classes of relevant information and their value to the organisation.

13.3 Information classes

Information is to be classified according to the following criteria:

- Function (operational, management, strategic);
- Security (confidentiality, privacy, etc.); and
- Time (immediate, monthly, etc.).

The processing and management of data differs between these classes.

13.4 Information Value Network

An objective of the IA is to define the sources of high-velocity information and ensure its availability and usage by the key business processes, enabled by the underlying applications architecture (AA) and technical architecture (TA). High-velocity information is that information which is shared along the information value chain of customers, suppliers, and partners in near real time, at both the transaction and decision support levels, to maximise operational efficiency and competitive advantage.

The value of information

(*Infonomics*) is determined by the competitive advantage gained by the use of the information product. It is the price premium that the consumer of information is willing to pay that exceeds the extra cost of providing the information product. There are essentially three dimensions of information value (*velocity, density and reach*) and the value of information can be increased by moving along one or more of these dimensions.

Methods and tools such as "information value network analysis" are used to diagnose problems or uncover opportunities to leverage information technology to create high value, low cost linkages with external parties and across the lines of business (LOB). The information value network describes the linkages in the network and the value of the information across the business value chain. Since



information is an artefact of business processes, it surrounds and supports the physical value chain.

U.R.

Gap Analysis

U. R.

14 Gap Analysis

Gap analysis will assist

A gap analysis is used in the context of **EA** to **identify differences between two states of an EA**. Formal models of an EA allow tool support and the visual representation of these models.

14.1 Steps

This was achieved through:

- Identifying the current situation and defining what is important for PKSDM;
- Setting S.M.A.R.T goals of where you want to end up;
- Analysing gaps from where PKSDM is to where it wants to be; and
- Establishing a plan to close existing gaps.

14.2 Matrix

14.2.1 Business Requirements

Requirement (Future State)	Action	Deliverables	Responsibility	Status	Target date
BAR1 Enable the rationalisation of core business processes across the organisation	Modelling training Modelling tools selection and training Model key business processes Analyse /rationalise models	Defined modelling methodology Skilled business technologists Current and future state business models	ICT		
BAR2 Ensure that organisational roles and responsibilities are defined	Obtain/define organisational roles and responsibilities for key business processes	Defined roles and responsibilities (in Organisation Architecture)	ICT/Bus		
BAR3 Enable effective transition planning and co-ordination	Conduct gap analyses Determine migration plans Prepare Implementation plan	Gap assessment Migration plan Implementation plan	ICT/Bus		
BAR4 Enable the streamlining and automation of core business	Refer BAR1				

U.R.

Requirement (Future State)	Action	Deliverables	Responsibility	Status	Target date
processes across functions					
BAR5 Ensure that Human Resource planning process is accommodated	Incorporate HR plan in Organisation Architecture	HR plan incorporated into Organisation architecture	ICT/HR Bus unit		
BAR6 Ensure that a business Research and Development function is accommodated	Research R & D best practices. Present proposal to business. Incorporate identified R & D roles, responsibilities, functions and processes into Organisation Architecture	R & D Proposal Defined R & D functions/ processes incorporated into Organisation Architecture	ICT and All Bus units		
BAR7 Enable the definition, analysis and segmentation of the customer base	Define customer base Incorporate into Data Warehouse environment	Defined customer base. Customer database (in DW)	Bus units and ICT		
BAR8 Ensure the provision of adequate and appropriate service delivery mechanisms	Define required services. Identify/rationalise service delivery channels and mechanisms. Project(s) to be identified to develop /implement channels /mechanisms	Defined service delivery channels and mechanisms mapped to customer base	Bus units and ICT		
BAR9 Enable differentiated service pricing mechanisms where appropriate and required	Determine costs of services Determine market prices Price services Project(s) to be identified to enhance billing system	Service delivery pricing schedule Architecture Project Requirement	ICT and Bus units		
BAR10 Ensure the identification and currency of benchmark standards	Define service delivery Measurement criteria Identify sources of, and obtain, service delivery benchmarks	Service delivery measurement criteria Identified sources Implemented process	ICT and Bus units		

h R

Requirement (Future State)	Action	Deliverables	Responsibility	Status	Target date
	Develop process to maintain currency of benchmarks				
BAR11 Ensure appropriate service delivery control mechanisms are identified and implemented	Identify appropriate service delivery control and monitoring mechanisms. Project/s to be identified to enable the mechanisms.	Enabled control and Monitoring mechanisms (applications, procedures, etc.)	ICT		
BAR12 Ensure that appropriate information management policies are institutionalised	Define and implement the Communication strategy and policy. Define and implement information management policies and procedures through the IA.	Communication strategy and policy. Information Management Policies and Procedures	ICT		
BAR13 Enterprise architecture development must be cost-effective	Deliver just enough just in time. Measure the contribution of EA to the achievement of the corporate goals	Defined Metrics Defined Measurement process/guideline	ICT		
BAR14 Ensure the implementation of performance measurement and evaluation mechanisms for management and public representatives	Refer to BAR10 & BAR11 Business to define measurement criteria				
Outstanding from BA business policies, principles guidelines and standards document	Develop policies, principles, guidelines and standards	1 Business technologist job description 2 Strategic planning forum roles and responsibilities 3 Strategic planning guideline 4 Identified corporate communication standards and guidelines 5 Enterprise modelling	ICT ICT/Bus ICT Communication and ICT departments ICT ICT		

Requirement (Future State)	Action	Deliverables	Responsibility	Status	Target date
		standards and guidelines 10 Architecture conformance checklist 12 Architecture organisation and governance.	ICT		

14.2.2 Information Requirements

Requirement (Future State)	Action	Deliverables	Responsibility
IR1 Eradicate uncontrolled data duplication and redundancy	Project to be initiated	- Project Scope. - Migration plan.	IA
IR2 Introduce standards, controls and procedures to ensure the accuracy and integrity of information.	Develop the standards and guidelines as identified in the Information Policies, Principles, Guidelines and Standards document	- Corporate communication standards and guidelines - Modelling standards and guidelines - Architecture Repository Specification - Change management procedures - Data administration procedure - Corporate data processing guidelines - Reviewed disaster recovery procedure - Reviewed Internet policy	IA
IR3 Catalogue/define and document corporate information sources (internal and external).	Schedule workshop with business	Populated Catalogue of Authentic Information sources	IA
IR4 Classify corporate information according to specified criteria (e.g. function, security, time, strategic value, etc).	a. Specify criteria. b. Populate metadata repository.	Repository populated with information.	IA
IR5 Ensure that users can trigger workflow processes from one	a. Define metadata model.	Metadata ERD.	IA TA

Requirement (Future State)	Action	Deliverables	Responsibility
business unit to the other	b. Establish metadata repository. c. Populate metadata repository. d. Incorporate metadata guidelines in Corporate Data Processing guidelines. e. Ensure data management standards and guidelines are applied.	- Functional specification for metadata repository. - Repository populated with metadata. - Quality assurance procedure	
IR6 Ensure that all documents created have version control	Initiate electronic records and management system	- General workflows - Transactional workflows	TA
IR7 Ensure that standard response times are triggered	Manage response times by users in the value chain	- Workflows should not sit in inbox for more than 48 hrs - System notification to supervisors	TA
IR9 Ensure that information is integrated across common business subjects. (E.g. Customer).	a. Project to be initiated. b. Define the common business subject areas.	- Common business subjects. - Project Scope. - Migration plan.	IA BA
IR10 Ensure that management information is readily available and accessible through a controlled MIS environment.	a. Define the MIS b. Environment c. Initiate project	- MIS environment - described within the - Corporate Data Processing Guidelines. - Project Scope. - Migration plan.	IA AA TA
IR12 Ensure that the data architecture is structured to enable flexibility	Apply best practices and principles	Incorporated in deliverables of IR2	IA and TA
IR13 Ensure that service delivery management information is readily available through a controlled MIS environment.	Refer IR10		IA AA TA

U.R.

Requirement (Future State)	Action	Deliverables	Responsibility
IR14 Enable the provision access to information and data according to differing requirements in a managed and controlled environment.	Apply best practices and principles	Incorporated deliverables of IR2 in	IA AA TA
IR15 Enterprise architecture development must be cost-effective	a. "Deliver just enough just in time" b. 2) Measure the contribution of IA to the achievement of the corporate goals	- Metrics definition - Measurement process/guideline	IA
IR16 Ensure controlled access to information by the general public via appropriate media and channels.	a. Classify information b. Apply sound data management principles accordingly	Refer IR2, IR4 and IR5	AA and IA
IR17 Ensure that management and public representatives have controlled access to information required for effective and rapid decision making.	Refer IR16		AA and IA



Enterprise Architecture (EA)

C.R.

15.1 Purpose and Scope

This Information Management Policy document is a consolidation of all policies and procedures pertaining to the management of corporate information within PKSDM Administration (hereinafter referred to as Administration). Based on the Information Architecture (IA) principles as contained in the Information policies, principles, guidelines and standards document, these policies are an integral component of the overall Information Architecture (IA) and cover:

- i. Information governance processes to support information management principles and practices that address: security access, privacy/confidentiality, information quality, integrity, authenticity, archival cycles, business continuity planning, and ownership;
- ii. Information management deliverables that address roles, responsibilities and organisation structure for managing information content and delivery (e.g. *information custodian (steward), owner and user*).

The purpose of the document is to set out the Information Management Policy for the Administration so as to enable the policy to be understood by all concerned and effectively applied throughout PKSDM. This policy incorporates the contents of the requirements as extracted from the business units, particularly communication, which it now supersedes.

Figure 13: below reflects the logical structure of the policies and procedures:

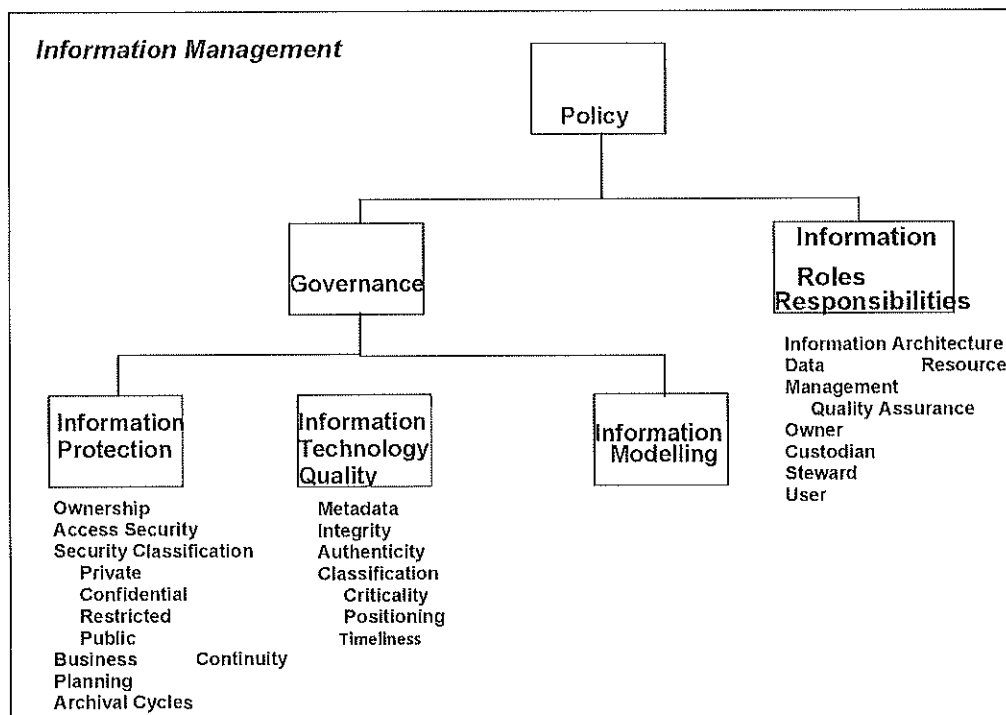


Figure 13: Information Management

15.2 Definitions

The term “data” generally refers to all stored data facts (primarily, but not limited to, those which are stored electronically in digital, machine-readable form), and “information” generally refers to data which has been processed to become meaningful.

Throughout this document, the term “information” must be understood to include both **data** and **information** and furthermore, to include all types of information whether textual, spatial, imaged, voice, video and objects.

Corporate information refers to all information used in the management and operation of the PKSDM.

15.3 Objectives

The objectives of the Information Management Policy are to ensure:

U.R.M.

- i. a common vision and acceptance of the scope and nature of information management within the Administration;
- ii. that information, a valuable resource of this Administration, is managed and controlled properly thereby minimising the risk of incorrect decision making as a result of invalid information;
- iii. that information is protected according to adequate security measures;
- iv. that adequate and up to date metadata (data about data) is maintained;
- v. that the quality of information is always compliant with EA standards; and
- vi. that authorised personnel in the Administration and all stakeholders are able to use information to its full potential.

15.4 Applicability

This policy addresses the use of information as a corporate resource and is therefore applicable to the PKSDM including all its business units and stakeholders.

16 Approach and Philosophy

The approach and general philosophy of the Information Management Policy of the Administration is based on the following basic principles:

- i. Information is a corporate resource, and therefore the only owner of this resource is the Administration itself;
- ii. Management of the information resources will be a cooperative effort between the information users within the Administration, senior management and Information and Communication Technology (ICT);
- iii. No one will attempt to use information in such a way that it will benefit one small part of the Administration at the expense of the entire Administration;
- iv. From the foregoing it is clear that no individual person, Section, or Department is the owner of a particular piece of information. However, owners must be assigned for every information subject area, where such ownership will involve responsibility for creation, maintenance, deletion or integrity, or a combination of these, of the subject area involved;



- v. The Administration, as well as the individuals serving the Administration, will regard and manage information resources as critical to the fulfilment of its mission and will therefore give full support in adhering to this Information Management Policy;
- vi. The Administration will exploit and utilise its data and information resources to the maximum extent to avoid duplication or wasteful and unnecessary expenditure of human, financial, material, or equipment resources and to increase the efficiency and effectiveness of the Administration in fulfilling its mission and objectives; and
- vii. The Administration will also seek and exploit opportunities to utilise information to generate revenue, add value to products and services, reduce and avoid costs, meet customer needs and achieve strategic advantages.

17 Information Governance

This part of the policy defines the information governance processes required to ensure that information is protected, information quality is maintained and that information is modelled according to the EA modelling standards.

The policy statements contained herein are formulated in order to support the principles identified in the IA.

17.1 Information Protection

All information shared across the enterprise is regarded as corporate information and therefore must be managed accordingly. Data and information must be protected according to best practice security policies and procedures. These must cover the following:

- i. Ownership
- ii. Security Classification
- iii. Access Security
 - Information Access
 - Network Access



- Remote Access
- iv. Business Continuity Planning
- v. Virus Protection

17.1.1 Ownership

Definition

Ownership defines the exclusive rights conferred on certain individuals or groups of individuals in terms of managing information. The categories of ownership are as follows:

i. Owner

The owner has the overall responsibility for funding the development and maintenance of the information asset, deciding on its security classification and allocating access rights.

ii. Custodian

The custodian (also referred to as “steward”) is responsible for controlling the use and protection of the information asset on behalf of the owner and in accordance with the owner’s instructions.

iii. User

The user is an individual who has been authorised by the owner of the information asset to access and/or update the information.

Policy Statements

Owner

- i. All information is owned by the PKSDM, and is therefore a common shareable resource referred to as corporate information;
- ii. Information will be captured by the user(s) or Business Unit that is in the best position to do so, regardless of subsequent value or use by the user(s) or Business Unit; and
- iii. The Municipal Manager (**MM**), the Executive Management Team and other staff of the PKSDM, will be accountable for:

- a. Information modelling and planning processes;

U. N.

- b. Funding and maintaining an appropriate organisation structure, skills base and technical infrastructure, related to the management, use and modelling of information;
 - c. Resolution of policy and procedural issues in a timely and effective manner;
 - d. Resolution of conflict between user(s) and/or customer interests; and
 - e. Identifying and appointing owners for each information subject area.
- iv. An appropriate funding strategy must be implemented to ensure that:
 - a. Common, shared information resources are developed, acquired and utilised. This will eliminate financial or political disincentives to the sharing of information resources within the PKSDM;
 - b. The maintenance of information resources, which are not of a shareable nature, will be funded from an appropriate user funding source, depending upon the primary beneficiary or user of the information resource.
- v. The owner is responsible for determining the security classification of the information under his/her control and the granting and revoking of access rights to individuals or groups.
- vi. The owner is responsible for the overall integrity of the information.

Custodian

- i. The ICT is, by default, the overall custodian of all PKSDM corporate information assets. Exceptions to this must be handled through the owner.



- ii. The custodian is responsible for controlling the use and protection of the information asset on behalf of the owner and in accordance with the owner's instructions.

User

Users of information within the PKSDM will be held accountable for:

- a. Correctly and unambiguously defining information requirements;
- b. Accepting all information in strict confidence, and not disclosing or reproducing it in any manner, form or way, except as directed by the management of the Administration and according to security classification limitations.

Procedures

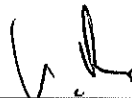
- i. Request for information access rights must be completed on the prescribed forms and logged via the ICT Co-ordinator for further processing;
- ii. Owners and custodians must be appointed through the ICT/Architecture Review Board;
- iii. The ICT System Administrator or his delegate is to maintain a register of identified owners and custodians.

17.1.2 Security Classification

Definition

All information will be classified for security purposes into one of the following security categories:

- i. **Confidential** information is of a very sensitive nature and which should be given special protection. Access rights will be assigned on a need-to-know basis and will be update-protected;



- ii. **Restricted** information is not available to the public (customers and interested persons). Access rights will be assigned on a need-to-know basis and will be update-protected; and
- iii. **Public** information will be freely accessible to individuals or groups of individuals within the PKSDM and to the community at large and which will be update-protected.

Policy Statements

- i. Official reports to PKSDM will be classified as follows:
 - a. All "**yellow**" papers are regarded as confidential;
 - b. All "**green**" papers are regarded as restricted; and
 - c. All "**white**" papers are regarded as public.
- ii. By default, all unclassified information will be regarded as public.
- iii. All access to restricted and confidential information must be authorised and must conform to Access Security policies as defined below.
- iv. No private or personal information is to be stored on the PKSDM's resources.

Procedures

All information to be classified must be classified by the appointed owner.

17.1.3 Access Security

Definition

Access security can be divided into three types of access, namely Information Access, Network Access and Remote Access.

Policy Statements

- i. All access to corporate information must be centrally administered;
- ii. Access to corporate information must be granted by the owner; and
- iii. Once an individual has left the employment of the PKSDM, ICT Systems Administrator must ensure that all access rights the individual had to corporate information, are revoked.



17.1.3.1 Information Access

Definition

Information can only be accessed by certain individuals or groups of individuals who have been granted the required authority. This in turn ensures that databases are protected against all internal and external risks.

Policy Statements

- i. Information access and update rights must be centrally administered by a Database Administration or ICT Systems Administrator's delegate;
- ii. User access to databases will be controlled via standard profiles aligned with user access rights;
- iii. All additions, changes and deletions of information must be auditable.
- iv. A standard set of protection measures will be defined for each security classification to ensure consistency in the implementation of security once information has been classified and to save time and effort on development projects;
- v. The PKSDM shall actively prosecute the theft, misuse or inappropriate disclosure of its information. Use of information for other than work-related purposes will be considered misuse; access or update by a person who is not formally authorised to do so will be considered as theft; and
- vi. If a user does not access the database for a period of time (to be determined), the user's access rights must be terminated.

Procedures

Requests for access to information must be submitted on the prescribed form (as provide for by PAIA to the owner for authorisation and then to the Database Administration for implementation.

17.1.3.2 Network Access

Definition

Network access ensures the effective use of communication network facilities in a secure environment. If there is insufficient control over network

connections, it is quite possible that unexpected entry points to the network may occur. This will allow unauthorised access to the computer infrastructure and the communication network, thereby putting information at risk.

Policy Statements

- i. Access to the corporate communication networks and information systems may be restricted to those with a genuine need to conduct PKSDM business;
- ii. Active Directory Service will be implemented to manage, authenticate users and distribution of patches;
- iii. All terminals and information systems, connected to the corporate communication networks, must be identified and classified;
- iv. Each individual will be uniquely identified to the processing environment by means of a unique, protected password. The individual is responsible for maintaining the secrecy of his/her password;
- v. User access to the network, servers, applications, and files will be controlled via standard profiles aligned with user access rights.
- vi. Administrator rights on production servers should be limited to identified support personnel only;
- vii. Administrators/support personnel must change their passwords regularly to ensure that the servers are not compromised by unauthorised access from insiders and outsiders;
- viii. If a user does not access the system for a period of time (to be determined), the user's access should be terminated;
- ix. Users should not be able to sign onto more than one workstation at a time;
- x. Owners and custodians are responsible for the security and use of terminals and network devices under their jurisdiction; and
- xi. Support Division reserves the right to monitor any network traffic as and when necessary.

Procedures

Requests for access to the network must be submitted to the ICT Systems Administrator for authorisation and implementation.

C. R.

17.1.3.3 Remote Access

Definition

Remote Access to the network is typically by dial-up facilities, e.g. telephone, mobile phones, modem, etc. Secure and resilient remote access is required so as not to compromise the confidentiality, integrity and availability of PKSDM information and information systems.

Policy Statements

- i. ICT Systems Administrator authorised remote users will be restricted to the minimum services and functions necessary for fulfilling their work requirements (excluding Internet);
- ii. The confidentiality and integrity of PKSDM information will be protected over remote access connections. The level of protection required will be determined by the assessed risk;
- iii. Remote users may only access information systems using software supplied or approved by ICT. An approved minimum standard configuration of hardware and software will be employed;
- iv. External access to communication networks must include strict identification, authorisation and authentication procedures; and
- v. ICT reserves the right to monitor any remote access logs as and when necessary.

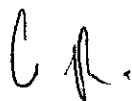
Procedures

All remote users must sign and adhere to a code of conduct which covers their responsibilities in terms of remote security.

17.1.4 Business Continuity Planning (BCP)

Definition

Business Continuity Planning (BCP) is the process of planning for the resumption of critical business operations following an unavoidable mishap or



disaster. It includes precautionary measures to ensure that information is secure, as well as procedures to restore information. These include:

- Archiving;
- Backup and Recovery (including versioning); and
- Disaster recovery.

Policy Statements

- i. All information stores will be subject to regular backup, recovery and offsite storage procedures to ensure recovery in the case of the destruction of information;
- ii. Backups will now be done on cloud storage;
- iii. Backups will be subjected to regular audits and testing; and
- iv. Data archiving must be scheduled to run according to predefined events.

Procedures

A Disaster Recovery procedure must be kept up-to-date as part of the change management process. (To be defined).

17.1.5 Virus Protection

Definition

Computer Virus protection is necessary to ensure that newly released viruses do not destroy the confidentiality, integrity and availability of the PKSDM's information.

a) Policy Statements

- i. All workstations and servers, running operating systems and services that can be affected by viruses, must be protected by the ICT approved Anti-Virus software;
- ii. Anti-Virus software must be kept up-to-date at all times;

U. R.

- iii. Virus alerts to PKSDM staff are only to be sent out by ICT Systems Administrator and NOT by end users. Users are to forward alerts received from external parties to ICT Systems Administrator only;
- iv. A mechanism needs to be put in place to filter out known viruses from incoming mail;
- v. Users must practice due diligence by reading ALL internal virus alerts sent out from the ICT Systems Administrator and adhere to the instructions given in these alerts; and
- vi. ICT Systems Administrator reserves the right to monitor any logs as and when necessary.

Procedures

Users must ensure that the latest version of the ICT approved anti-virus protection software is loaded and active on their workstations.

17.2 Information Quality

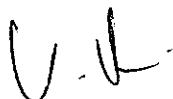
The quality of information must be governed according to best practice policies and procedures. These must cover the following:

- i. Metadata
- ii. Integrity/Authenticity
- iii. Classification
 - Criticality
 - Timeliness
 - Positioning
 - Security

17.2.1 Metadata

Definition

Metadata is data about actual data and is required to identify and enhance the management and sharing of corporate information. Examples of metadata include data element descriptions, data type descriptions, attribute and property descriptions, range and domain descriptions, and process and method descriptions. The repository environment encompasses all corporate metadata



resources, database catalogues, data dictionaries, and navigation services. Metadata is stored in a data dictionary and repository, and insulates the data warehouse from changes in the scheme of operational systems.

Policy Statements

- i. Metadata must be defined for all corporate information and must be made accessible to all authorised stakeholders;
- ii. Metadata must as a minimum include the following: information source, owner, custodian, functional classification, security classification, subject area, standard definition, required format and original date created.

Procedures

The ICT Systems Administrator must define the data, classify and assign the responsibilities within PKSDM.

17.2.2 Integrity/Authenticity

Definition

Integrity of information is the assurance that all information is true, correct and accurately reflects reality.

Policy Statements

- i. All database designs must be quality assured to ensure that integrity is maintained;
- ii. All information models must be quality assured and formal change management procedures effected to ensure the accuracy of the models.
- iii. A formal 3rd party review of information models must be conducted on an annual basis to ensure that models are kept up-to-date;
- iv. All transactions which change the database (create, update or delete) will be designed, constructed and maintained in such a way as to preserve the integrity of information;
- v. Users must exercise due diligence when capturing data to ensure that the data accurately reflects reality;
- vi. Standard information access mechanisms must be utilised;

V. R.

- vii. Information must be captured once only to avoid duplication;
- viii. Information may be replicated under controlled circumstances only;
- ix. Information must be validated and corrected at source;
- x. Information will be captured as near to the true source of origin (both from a geographic and time perspective) as possible and will be validated and entered into the database as directly as possible to minimise use of paperwork and other interim handling procedures;
- xi. Data naming and formatting standards must be adhered to;
- xii. Redundant data must be archived and removed; and
- xiii. Formal change control procedures must be adhered to.

Procedures

To assist in managing information integrity, three distinct information/application environments will be established and maintained as follows:

- i. **Development:** Programs and information in this environment will be essentially controlled by the Development Division and will be used during the development process;
- ii. **Test/acceptance:** Programs and information in this environment will be strictly controlled by the custodians, as this environment will be for controlled exercising and acceptance testing by users. Information values will be well designed to ensure predictable and verifiable test results. Changes to information values will be made only by means of controlled logical transactions, not through ad hoc updates. Development staff will not make direct changes to programs or information structures in this environment; and
- iii. **Production:** Programs and information in this environment will be strictly controlled by the custodians, as this will be the live processing environment on which the Administration's daily business will depend. Changes to information will only be allowed through controlled logical transactions, never through ad hoc updates. No direct changes to



programs or information structures will be allowed in this environment.
Only authorised users will be allowed access to this environment.

17.2.3 Classification

Definition

The classification of information will determine how it is managed and controlled. Required classifications are:

- i. **Criticality**, which refers to the extent to which PKSDM is dependent on the information for its effective operation;
- ii. **Timeliness** of information, which refers to how soon information becomes available after an event has occurred;
- iii. **Positioning**, which refers to whether the information is classified as operational, management or strategic; and
- iv. **Security** (refer to 3.1 Information Protection above).

Policy Statements

- i. All critical information must be identified and managed and protected accordingly;
- ii. The timeliness of information will be determined on a cost/benefit basis;
- iii. Information will be made available as timely as is possible and practicable according to the users' requirements; and
- iv. Operational, Management and Strategic information will be logically separated and managed accordingly.

Procedures

Adhere to the Data and Data Warehouse domain principles, procedures and guidelines.



17.3 Information Modelling

Definition

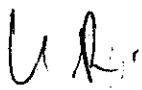
An information model represents information in an understandable simplified format.

Policy Statements

- i. PKSDM will create and continually maintain graphical models of corporate information, both current and future;
- ii. Information must be modelled according to the Enterprise Architecture Modelling Guidelines and the Application Development guidelines and will incorporate;
- iii. Information Value Network Model;
- iv. A Corporate Information Model;
- v. Subject Area Data Models where one Data Model will exist for each Subject Area;
- vi. Logical Data Models, where one Data Model will exist for each computerised system;
- vii. Physical Data Models, where each Data Model will correspond to a Logical Data Model; and
- viii. Whenever vendor-supplied application packages are evaluated, it must be done against, *inter alia*, the conceptual data models which already exist. The costs of remedying or managing all inconsistencies (including duplicated data files, reformatting, changing file designs or program logic, building data interfaces, etc) will be identified, quantified and included in the projected cost of implementing any vendor-supplied option before acquisition decisions are made.

Procedures

Adhere to the Information Modelling principles and guidelines as defined by the ICT within the EA.



18 Information Management Roles and Responsibilities

This part of the policy defines the roles, responsibilities and organisation structure required to implement the policy statements contained in this document. It defines, *inter alia*, the role that users will play in being custodians of information; the role that the ICT will play through the Data Resource Management section and the Information Architecture section, and the role that these sections will play in ensuring that this policy is understood, adhered to and effectively applied. The RACI will be clearly defined in the master document.

These entities can be classified under the following groupings:

- i. Information Architecture;
- ii. Data Resource Management;
- iii. Owner;
- iv. Custodian;
- v. User;
- vi. Architecture Review Board;

18.1 Information Architecture

Role

The Information Architect is responsible for defining the Information Architecture Strategy which establishes the value and importance of using information effectively across lines of business, as well as the need to achieve collaborative excellence with external partners and customers. This includes:

- i. modelling the "information supply chain or network" extension of the Enterprise Business Architecture (EBA) to enable rapid business decision making and information sharing;
- ii. establishing information governance processes to ensure the quality, integrity and security of corporate information assets; and
- iii. defining roles, responsibilities and organisation structure for managing information content and delivery.

U. R.

Responsibilities

- i. Establish communication and enforce a governance framework to coordinate and collaborate with suppliers/partners, employees, stakeholders, and customers in business activities across the enterprise value network;
- ii. Establish the relevance of information and data within the context of business strategies, goals, and objectives;
- iii. Classify business information, in terms of its value to the enterprise, to ensure information sharing between LOB's, trading partners, and regulatory bodies;
- iv. Establish information security access, privacy, confidentiality, quality, integrity, authenticity, and archival cycles;
- v. Provide a foundation for the development and endorsement of common or standard data definitions.
- vi. Ensure information access and sharing supports physical value chain and information value network;
- vii. Ensure information compliance within audit and legal requirements;
- viii. Ongoing development of the Information Architecture (IA) framework.
- ix. Identify Business Information Requirements (BIR) in conjunction with the business and catalogue in the information products catalogue;
- x. Optimise information value chains/networks across the enterprise in conjunction with the business and identify opportunities for reuse;
- xi. Identify opportunities for digital innovation and give input to the TA group;
- xii. Determine what metrics will be used to measure information sharing success in conjunction with the business. (e.g. revenue increase, cost decrease, reduced service delivery times, etc.);
- xiii. Identify MIS and Data Warehouse application needs;
- xiv. Give input to the planning of application portfolios;
- xv. Conduct gap analysis between the current and future states of the Information Architecture and give input to the migration planning process;

U, R,

- xvi. Perform conceptual information system design; and
- xvii. Responsible for the development of information models.

18.2 Data Resource Management

Role

The Data Resource Management (DRM) group functions as a separate entity and their main function is to oversee the operation and application of this Policy. Whereas the Information Architecture group are the policy makers, DRM group are the policy enforcers. Additionally the DRM group provides data analysis support in IS development.

Responsibilities

- i. Catalogue authentic sources of information in terms of who has the information on, in what form, who owns/manages it, how it should be leveraged;
- ii. Create and maintain the metadata (including models) in a suitable repository for the organisation;
- iii. Document the use and definition of information items (e.g. service, consumption, customer, etc.);
- iv. Maintain and administer the DRM standards, procedures and guidelines and link to the Technical Architecture;
- v. Provide training and support as regards the content and operation of the DRM standards, procedures and guidelines;
- vi. Keep abreast of all changes in terms of business strategy, enterprise architecture and systems development;
- vii. Identify any matters of conflict involving the use of, and changes to, information resources and escalate to the Information Architecture group;
- viii. The DRM group is the custodian of the various information models and will ensure that they are initially created; and
- ix. Ensure that change control procedures are in place to ensure the accuracy of the information models and the quality assurance thereof.

U. R.

18.3 Owner

- i. Refer to the policy statements as defined for Owner in section 3.1.1
- ii. Ownership elsewhere in this document.

18.4 Custodian

- i. Refer to the policy statements as defined for Custodian in section 3.1.1
- ii. Ownership elsewhere in this document.

18.5 User

- i. Refer to the policy statements as defined for User in section 3.1.1
- ii. Ownership elsewhere in this document.

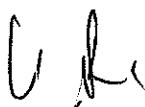
18.6 Architecture Review Board.

Role

The Architecture Review Board is responsible for providing input for and reviewing and approving the deliverables for the Information Architecture.

Responsibilities

- i. Collaborate in developing and the conceptual architecture;
- ii. "Ambassadors" of architecture throughout the business units;
- iii. Reviews and approves the defined policies, procedures, standards and guidelines; and
- iv. Denies/Approves exceptions to the defined policies, procedures, standards and guidelines.



Enterprise Architecture Roadmap

U.R.

19 The Enterprise Architecture Roadmap

The Roadmap lists recommendations and ICT requirements which will enable the realisation of the vision and milestones set above. The following critical success factors were taken into account when developing and sequencing the roadmap.

19.1 Business/ICT Alignment

The Business/ICT alignment places the PKSDM ICT Strategic Plan in context, identifies internal and strategic drivers, establishes the PKSDM strategic objectives, formulates the PKSDM ICT guiding principles and defines ICT Strategic Plan risks.

The PKSDM ICT Strategic Plan provides a conceptual view of the required state of PKSDM ICT to support the business objectives, and the role envisaged for the ICT unit in the various dimensions

19.2 Drivers and Objectives

The ICT Strategic Plan drivers, as indicated in the figure below, are formulated from the PKSDM strategic objectives, external ICT trends and Government best practices.



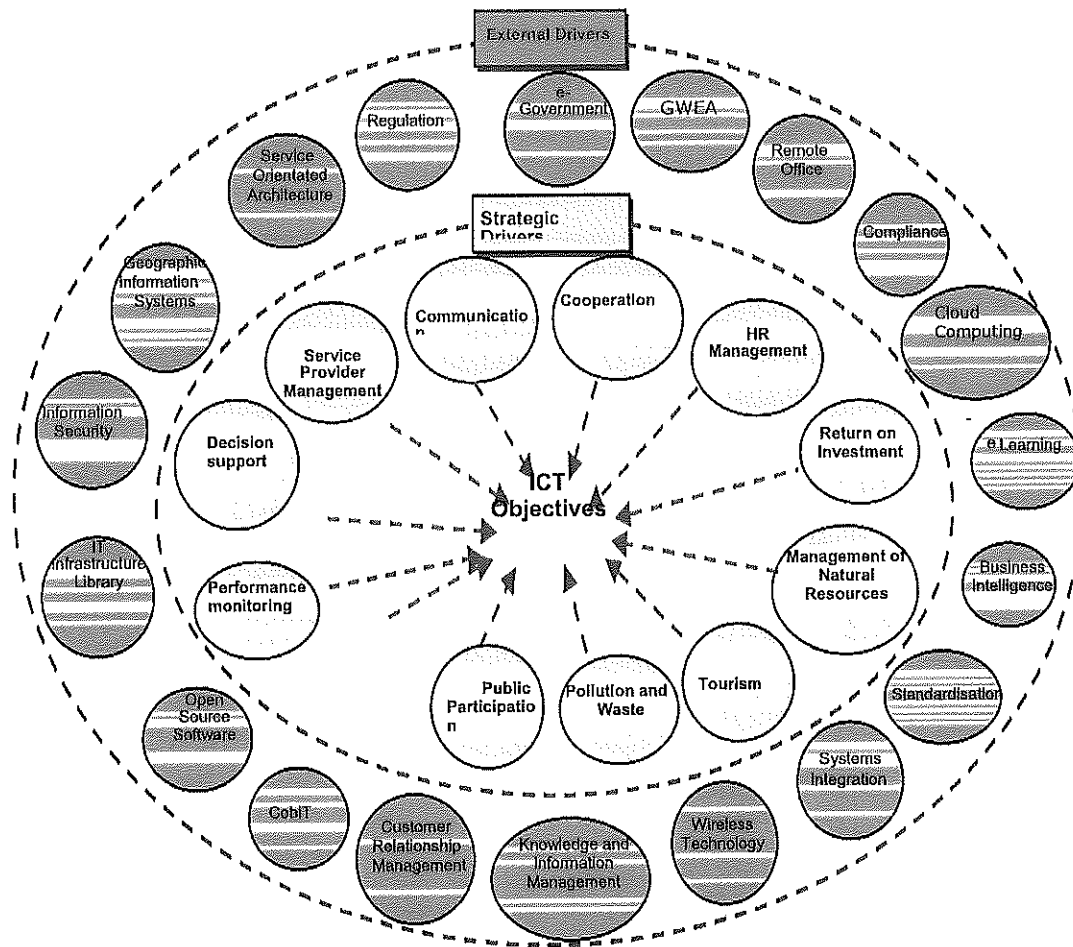


Figure 14: ICT Strategic Drivers

Trend	Short description
GIS	Software application that provides a visual representation of geographic and demographic data. GISs are also capable of modelling and layering both demographic and geographic information. ICT allows the query or analysis of GIS data and receives the results in the form of some kind of map.
SOA	SOA is gradually replacing monolithic architecture as the premier design principle for new business applications. ICT emphasizes loose coupling between software components, and in its use of separately standing interfaces.
Regulation	A prescribed set of criteria and conditions which will include among other things, procedures, rules, specifications and standards for regulating and monitoring activities.

C.R.

Trend	Short description
e-Government	Electronic Government: Government activities that take place by digital processes over a computer network, usually the Internet, between the Government and Members of the public and entities in the private sector. ICT involves the electronic exchange of information to exchange products or services, to exchange information, or to complete financial transactions.
Remote office	In a fast-paced world connected by high speed networks, there is a trend towards working in a remote office as easily as in a central office. To cut on travel cost and time
Compliance	Regulatory compliance refers to the steps taken by organisations to ensure that personnel are aware of and take steps to comply with laws and regulations that apply to the organisation.
e-Learning	Learning facilitated and supported through the use of ICT.
Business Intelligence	BI is a broad category of application programs and technologies for gathering, storing, analyzing, and providing access to data to help enterprise users make better business decisions. BI applications include the activities of decision support, query and reporting, OLAP, statistical analysis, forecasting, and data mining.
Systems Integration	The art and science of integrating processes, functions, people and data so the end result is a seamless and tight knit system.
Wireless technology	Mobile ICT equipment, including cellular telephones, PDAs and the wireless networks that support connectivity in mobile use.
Standardisation	The process of establishing a technical standard for providing benefits of interoperability and greater efficiency.
CRM	An integrated information system that is used to plan, schedule and control all activities in an organisation dealing with its customer. ICT embraces aspects such as the call centre, marketing, technical support and field service.
COBIT	Control Objectives for Information and related Technology. A set of best practices (framework) for information (IT) management.
OSS	The source code of OSS is openly published, usually available at no charge, and often developed by voluntary efforts. For OSS licensed software the source code is distributed with the product, and the user is able to modify and redistribute derived works from this software.
ITIL	IT Infrastructure Library. A customisable framework of best practices that promote quality computing services in the ICT sector. These concepts support ICT service providers in the planning of consistent, documented, and repeatable processes that improve service delivery to the business.
Information security	The protection of information from unauthorized access (accidental or intentional), modification, destruction, or disclosure. Information security deals with several different trust aspects of information. Information security is not confined to computer systems, or to information in an electronic or machine-readable form. ICT applies to all aspects of safeguarding or protecting information or data, in whatever form.

G.R.

19.3 ICT Guiding Principles

In order to achieve its ICT objectives, the following ICT guiding principles define the manner in which PKSDM will conduct ICT activities. The ICT principles are a set of high-level organisation, information and technology “values” that will guide the PKSDM ICT unit in decision making.

19.3.1 Management, Organisation and Governance

- The ICT unit will work closely with the business to create an alignment between the business and ICT priorities;
- The ICT unit's primary focus is to align ICT priorities to business and the secondary focus is to align the PKSDM's initiatives to Government's larger ICT plans; and
- The ICT unit will take an active role in educating the business users of ICT systems and bring to the PKSDM business ideas on ICT-enabled opportunities.

19.3.2 Applications and Information

- The PKSDM will pursue packaged applications that achieve strategic value over those proven solutions which only lower risk;
- The PKSDM will use common solutions for core business processes across the business units, where ICT makes proven business sense;
- The PKSDM will strive for the optimal trade-off between business impact and effectiveness over ease of implementation;
- The PKSDM will pursue applications with business fit and functionality over technical considerations;
- The PKSDM will upgrade to new software versions, balancing the future value with ongoing software maintenance costs;
- The PKSDM will use strategic partnerships to access leading edge skills to accelerate implementation, however, the PKSDM will transfer this knowledge to its staff;

U.R.

- The PKSDM will make every effort to collect information once and maximise the sharing of that information element across relevant stakeholders;
- The PKSDM will use proven project and programme management approaches in pursuit of value; and
- The PKSDM will establish clear ownership of information and business applications amongst business units for the total life cycle thereof.

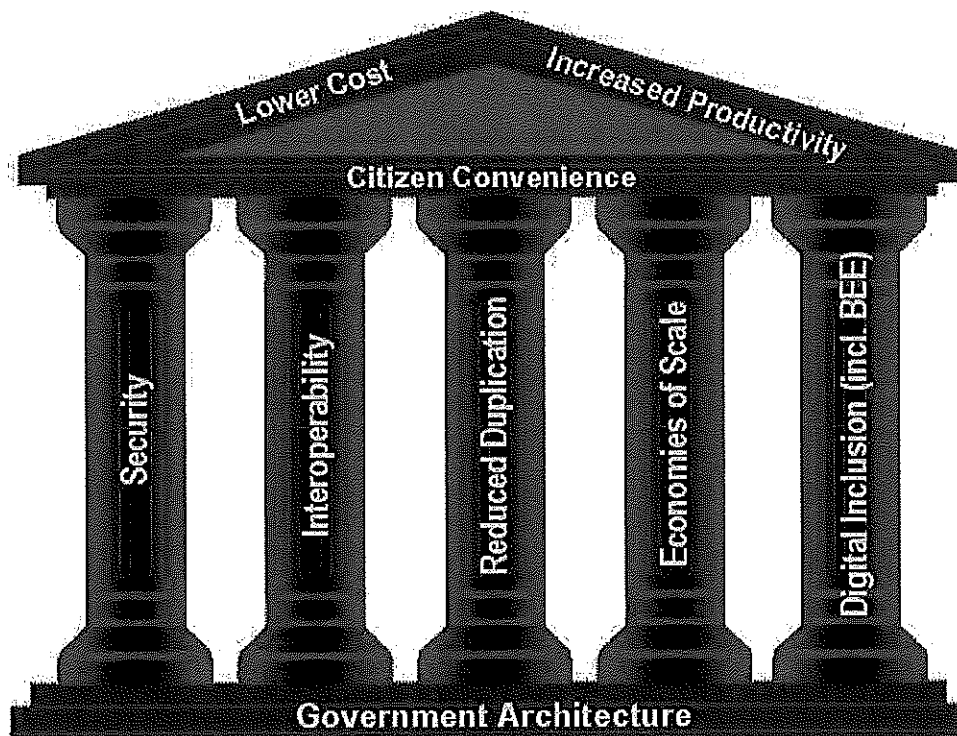
19.3.3 Architecture and infrastructure

- The PKSDM will physically and logically consolidate its servers for all systems;
- The PKSDM will standardise workstations/laptops/iPads, its operating systems and core application portfolios;
- The PKSDM will implement a common set of reusable infrastructure components across the organisation;
- The PKSDM will adopt security measures and standards that meet both Government and PKSDM requirements;
- ICT solutions identified should support the principles of interoperability, scalability and portability;
- The PKSDM will utilise open, vendor-neutral industry standards whenever possible; and
- The PKSDM will use a formal architecture management process.

19.4 Guiding Government's ICT efforts

ICT House of Values depicts the Government ICT House of Values, illustrating the main drivers of its ICT efforts. The primary objective of these concepts is to ultimately reduce ICT costs for Government, improve Government's efficiency and effectiveness and make ICT convenient for citizens to access Government services. It is imperative that the ICT organisation is positioned strategically to ensure that ICT receives the necessary exposure to enable the concepts embodied in the ICT House of Values.





The five "pillars" can be described as follows:

1	Security	Ensure that all products and services are secure and conform to the
2	Interoperability	Ensure that all ICT solutions integrate and are interoperable.
3	Reduced duplication	Ensure re-use and sharing of existing solutions.
4	Leverage Economies of Scale	Use Government's centralised buying power to procure ICT products and services.
5	Digital Inclusion	Ensure that the previously disadvantaged are empowered by: a) providing them with a cost-effective way of accessing PKSDM services via different channels – anywhere, anytime, anyhow; and b) providing them with training and overall skills development to understand and use the different channels available to them to access the PKSDM services.

U.R.

19.5 The ITM-IRM-IL Framework

The PKSDM ICT unit will fulfil its role primarily within three domains:

ITM	ITM includes the hardware, software, networks and applications needed to give the PKSDM access to its information, and automated business systems. ITM refers to managing the provision of services rather than actively providing the service. Managing includes the planning and organisation, and ensuring that the service is provided, as well as the monitoring of the service.
IRM	IRM focuses on the appropriate and optimal use of information and technology. Often the IRM role brackets the ICT role, in that ICT understands the business need, prepares the solution, and ensures that once the solution is implemented, the PKSDM derives the full benefits anticipated when the technology was initially justified.
IL	IL focuses on bringing the information and business process technology perspective to the leadership team. ICT is concerned with business direction, dimensions and boundaries.

The primary driving purpose behind ITM is to maintain Municipal momentum. The driving purpose behind IRM is to ensure optimum use of ICT and information. The primary driving purpose behind IL is to support the business direction and exploit enablement opportunities.

The ICT unit must play a dominant role within IRM and IL. Based on this premise as well as the assessment of the current ICT organisational structure, and the ICT organisational requirements indicated by the ICT Officer, the ICT organisation roles were mapped onto the ITM- IRM-IL model

19.6 Roles per ITM-IRM-IL framework

R	Responsible	This individual performs the work. The individual normally defines the business case and justification.
A	Accountable	This individual has the ability to make decisions. The individual approves the project. Financially responsible.
C	Consult	This individual is asked for their opinion. The individual may be the expert in the area. Information is obtained from them.
I	Inform	The outcomes of decisions are made known to this individual or group of individuals. The outcomes of these decisions will impact on the individual or group of individuals.

	Monitor services delivery
	Only part of ICT Management Role

C. R.

	Share with IRM Role
--	---------------------

Information Technology Management (ITM) highlights the RACI per ITO, ICT System Administrator/ICT respectively, according to the ITM-IRM-IL framework, main ICT domains and processes.

The RACI (R-Responsible, A-Accountable, C-Consulted, I-Informed) roles are defined below:

RACI analysis on IT/IM Roles vs. functionalities vs. processes							
Role	Main ICT domains and processes		IT/IM Functionaries				
			ITO	ITO	ITO	ITO	Management and Council
Information Technology Management (ITM)	Domains	Technical Support (Hardware/Software)					
		System technical support					
		System development and maintenance					
	Manage operational services delivery	Develop service delivery model	R	R	AI	C	I
		Match services to requirements	R	R	AI	C	I
		Organise service delivery capability	CI	R	AI	I	I
		Supply facilities supporting ICT environment	R	C	AI	C	I
		Report on ICT performance	R	R	AI	I	I
		Manage external services provision	A	R	AI	C	I
		Monitor services delivery	R	R	AI	C	I
	Manage ICT assets and Infrastructure	Obtain proposals/quotes	C	C	I	RA	I
		Evaluate vendor offerings	CA	R	I	C	I
		Procure services	C	C	C	RA	I
		Manage IM finance	C	C	C	RA	I
		Protect physical ICT assets	R	R	AC	R	I
		Manage ICT Inventory and assets	C	R	C	A	I
	Deploy Solutions	Identify departmental solutions set	CA		C	C	I
		Map department solution set to requirements	A		C	C	I
		Plan solutions implementation process	A		C	C	I
		Implement solutions	A		C	C	I
		Integrate new solution with service delivery model	A		C	C	I
		Educate and train users	A		C	C	I
		Define change control processes	A		C	C	I
		Develop and maintain procedures	A		C	C	I

U.R.

Information Results Management (IRM) highlights the RACI per ITO, ICT System Administrator/ICT respectively, according to the ITM-IRM-IL framework, main ICT domains and processes.

RACI analysis on IT/IM Roles vs. functionalities vs. processes							
Role	Main ICT domains and processes		IT/IM Functionaries				
			ITO	ITO	ITO	ITO	Management and Council
Information Results Management (IRM)	Domains	Key source of management information					
		System development and maintenance					
	Realise Solutions	Understand department strategic intent	A	R	C	C	I
		Understand branch strategic intent	A	R	C	C	I
		Translate strategic intent IM solutions	A	R	C	C	I
		Understand specific solutions requirements	CA	RA	C	C	I
		Define solutions	A	R	C	C	I
		Design solutions	A	R	C	C	I
		Construct and integrate solutions	A	R	C	C	I
		Test solutions	A	R	C	C	I
		Gain department acceptance and sign-off	A	R	C	C	I
	Manage information context	Facilitate information in business	R	C	A	I	I
		Provide context to information management	R	C	A	I	I
		Understand business processes	R	C	A	I	I
		Agree on IM facilitation role	R	C	A	I	I
		Structure information	R	C	A	I	I
		Manage information integrity	R	R	A	I	I
		Transform information	R	C	A	I	I
		Interpret results	R		A	I	I
		Communicate results and recommendations	R	C	A	I	I
		Institutionalise information transformation process	C	C	RA	I	I
	Manage IM quality	Define IM quality management framework/system	A	R	C	C	I
		Define IM quality processes and procedures	A	R	C	C	I
		Establish measures: CSFs, KPIs, standards	RA	C	C	I	I
Implement quality processes and measures		A	R	C	I	I	

C.R.

	Monitor quality management process	A	R	C	I	I
	Provide for Audit	A	R	A	I	I
	Manage IM Risks	R	R	A	I	I

RACI analysis on IT/IM Roles vs. functionalities vs. processes						
Role	Main ICT domains and processes		IT/IM Functionaries			
			ITO	ITO	ITO	Management and Council
Information Results Management (IRM)	Domain s	Key source of management information				
		System development and maintenance				
	Manage IM people	Develop IM skills portfolio	A	R	C	C
		Plan staffing requirements	R	C	A	C
		Manage internal transfer capabilities	R	C	A	C
		Recruit staff	R	C	A	C
		Place staff	R	C	A	C
		Provide career paths	R	C	A	C
		Develop staff	R	C	A	C
		Manage staff performance	R	R	A	I
	Manage IM ROI	Define IM ROI model	C	C	A	R
		Implement IM ROI model	C	C	A	R
		Manage IM ROI Model	C	C	A	R
		Communicate IM ROI performance	C	C	A	R
		Strategic justification	C	C	A	R
		Project financing	C	C	A	R
		Budget process	R	R	A	C
		Management accounting	C	C	A	R
	Provide (Client) IM Management system	Post implementation reviews	A	R	C	C
		Asset management	C	R	A	R
		Plan IM management system	A	R	C	C
		Implement IM management system	A	R	C	C
		Evaluate IM management system	A	R	C	C
		Govern IM conduct	R	C	A	C
		Operate IM Structure process	A	R	C	C

G.R.

Information Leadership (IL) highlights the RACI per ITO, ICT System Administrator/ICT respectively, according to the ITM-IRM-IL framework, main ICT domains and processes

RACI analysis on IT/IM Roles vs. functionalities vs.processes								
Role	Main ICT domains and processes		IT/IM Functionaries					
			ITO	ITO	ITO	ITO	Management and Council	
Information Leadership (IL)	Domains	Enhancing services delivery						
	Relationship management	Understand relationships	A	R	C	C	I	
		Market ITM-IRM-IL context, offerings and capabilities						
		Develop services levels per branch	A	R	C	C	I	
		Manage customer satisfaction	A	R	C	C	I	
		Proactively create new business capability	Understand the business strategy	R	C	A	C	I
	Define strategic IM drivers		A	R	C	C	I	
	Develop IL strategy		A	R	C	C	I	
	Tracking emerging technologies		A	R	C	C	I	
	Position the technologies		A	R	C	C	I	
	Map emerging technology to current and future applications		A	R	C	C	I	
	Create business case		A	R	C	C	I	
	Develop IRM strategy		A	R	C	C	I	
	Get buy in and educate the business		A	R	C	C	I	
	Communicate IM Strategies		A	R	C	C	I	
	Develop ICT strategy		A	R	C	C	I	
	Develop, implement and maintain architecture		Develop straw model department blueprint		R	I	C	I
			Define department blueprint	A	R	I	C	I
		Define branch blueprint	A	R	I	C	I	
		Define operational and technologies	A	R	I	C	I	
		Implement and maintain integrity	A	R	I	C	I	

C.L.

19.7 Roadmap Sequencing

The following summarise the basket of projects the municipality should embark on:

Application	Module	Functionality/Integration	Action plan
Office Automation		PKSDM utilises Microsoft platform and these applications support all other applications standardisation and ensures conformity and consistency in communication, storage etc. internally and externally.	Develop a design for a robust automation platform Upgrade the WiFi and server infrastructure to accommodate automated platform
Program and Project Management	Program Management	Program Management must give a single single-view of all projects. It must integrate to project management for the planning, scheduling and budgeting. Project management must integrate to supplier management, to ensure confirmation and availability all supplies. It must integrate to time management to keep track of the time utilised when delivering the project and cost of that time.	This is an urgent requirement and a Project Management Office must be established immediately because: 1. There is a dearth of readily available information on projects within the PKSDM. 2. No consolidated view of projects, their costs, progress, etc. 3. The next phase of this ICT project will require tight management.
	Planning and Scheduling	The phase will have as a large part of their mandate, the establishment and running of the PMO	The establishment and running of the PMO, as well as the knowledge transfer and training to the PKSDM staff.
	Execution and Measuring	All other projects can be brought under the discipline of the PMO once the capacity has been developed in-house	Implement project based approach for all municipal projects.

C.R.

Application	Module	Functionality/Integration	Action plan
Customer Relationship Management	Marketing Customer Development Opportunity Development Customer Services Stakeholder Management	The CRM application must integrate the marketing, customer development, opportunity development and customer services applications. including back office applications	Develop CRM requirements and perform a procurement selection process for the best fit CRM solution.
	IDMS (Integrated Document Management System)	1. This Document Management System must integrate with all applications and provide a centralized tool that manages document storage, sorting and retrieval in a view specified by the user. 2. Digital Signatures	1. Define the scope of information processing and storage for IDMS. 2. Assess the capabilities and limitations of the existing IMIS. 3. Extend the capabilities or replace IMIS with Microsoft SharePoint. 4. Procure and install to enable officials to authorise transactions by digitally signing on line while away from Municipality.
Supply Chain Management	1. Supplier Management 2. Tender Management 3. Contract Management 4. Inventory Management 5. Procurement Processing	The procurement application must integrate procurement, supplier management, asset management, vendor management, contract management and tender management. It must integrate to management accounting by linking the payments of contracts to cost centres and providing a transparent view of fund usage in the PKSDM.	Define information flows and processes for supply chain management. Perform a procurement selection process for the best fit SCM solution.
Asset Management		This Application must integrate with supply chain management system to	Define and implement an asset classification coding.

C. f.

Application	Module	Functionality/Integration	Action plan
		ensure real-time updates of the asset register	Perform a procurement selection process for the best fit asset management solution.
Management Information System		This application must link to all application and data to enable a consolidated view of all information for management decision making	Define the MIS requirement specification Perform a procurement selection process for the best fit MIS solution
Safety Health and Environment (SHE)	Hazardous Substance Dangerous Goods Regulatory Monitoring Occupational Health Waste Management Industrial Hygiene & Safety	SHE must integrate all different applications pertaining to hazardous substance, dangerous good, regulatory and monitoring, occupational health, waste management, industrial hygiene and safety. This broad integration ensures all tracking and documentation of regulatory requirements and activities as well as guidance documents. SHE integrates to all applications in the organization. In infrastructure development and maintenance it is critical for this integration to ensure non-abuse of hazardous substance, carrying of dangerous goods, as well as issues relating to waste management.	Define requirements specifications for: ▪ Hazardous Substance ▪ Dangerous Goods ▪ Regulatory Monitoring ▪ Occupational Health ▪ Waste Management ▪ Industrial Hygiene & Safety Perform a procurement selection process for the best fit SHE solution
GIS		The Geographical Information System (GIS) integrates to the project management tool set, utilities and Property management.	Define integration and reporting requirements. Develop and implement GIS integration.
Records Management		The records management system will support the registry where all organisation wide documentation will be catalogued and digitized. It must integrate to the IDMS.	Review and update the municipal file plan. Implement electronic filing aligned to updated file plan and integrated to IDMS.

C. K.

Application	Module	Functionality/Integration	Action plan
Property Management		Must integrate to the accounts receivable application, GIS and property information to ensure real-time updates of accounts when billing for services takes place Must integrate to the utilities management and customer services applications to allow for automated response to field services requests Must integrate to fleet management which reveals real-time information on all fleet used, and due for maintenance.	Define the property management requirement specification. Perform a procurement selection process for the best fit property management solution
Facilities/Utilities Management		The facilities and equipment management application will ensure the support of day-to-day operations of facilities and equipment managed by PKSDM.	Define the facilities management requirement specification. Perform a procurement selection process for the best fit facilities management solution.
Fleet Management		The application has to schedule facilities/equipment for usage, and prompt billing of facilities as well as store info on facilities/equipment location, maintenance record and usage	Define the fleet management requirement specification. Perform a procurement selection process for the best fit fleet management solution.
Enterprise Resource Planning (ERP)		ERP systems generally contain the modules that satisfy many of the functionality and requirements and integrate them all in one consolidated application. This eliminates duplication of functionality and data.	Review and define the functionalities that would require consolidation. Perform a procurement selection process for the best fit ERP solution.
Business Intelligence	Business Intelligence & Management Decision Support	This application must integrate to all information sources in the business that allows management to make informed decisions.	Perform a procurement selection process for the best fit business intelligence / decision support solution

Application	Module	Functionality/Integration	Action plan
	Knowledge Management	The knowledge management component must store all unstructured information. Anyone searching for information should be able to query the knowledge management database and find the information relevant to them	Perform a procurement selection process for the best fit Knowledge management solution
	Business Analytics	The business analytics component will store the structured information, and be able to provide information and reports on enterprise wide operations.	Perform a procurement selection process for the best fit business analytics solution
Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP)		The plan must ensure that it is possible to recover information/data across the municipality. The BCP must ensure that critical services are immediately restored	Define the risk appetite for information loss to the municipality Define the risk analysis specification for BCP and mitigation plan.
Risk Management		The risk management application must integrate to all applications in the business for risk analysis. It will mainly use data obtained by the Monitoring application for risk analysis but will require information from other applications as well.	Define the risk appetite for the municipality. Define the risk analysis specification. Procure and implement a risk analysis tool.

C.R.

Application	Module	Functionality/Integration	Action plan
Operational Audit	Audit Management Quality Control Quality Improvements	This Audit Management application must integrate to all other applications to access the relevant information during the auditing process. The Quality Control application must integrate to all other applications to access data for quality control to ensure efficiency, effectiveness and economic utilization of resources. The Quality Improvement application must integrate to the Quality Control application so that quality information can be shared for quality improvement purposes.	Define the audit charter and process. Develop specification to meet audit requirements and process. Perform a procurement selection process for the best fit audit solution.
Finance	Budgeting Management Accounting Treasury Expenses General Ledger Investment Management Accounts Payable Consolidated Financial Statements	The Finance application needs to integrate with external banking systems from which electronic statements, payments etc. will be obtained and reconciled with the internal systems.	The current Venus system must be ▪ Assessed for user friendliness and ease of use ▪ Secure and segregated access / functionality ▪ benchmarked against the reporting requirements for Finance for MSCOA compliance. ▪ Findings must be presented to EXCO for decision making on way forward.
Performance Management		The performance management application should integrate with finance, project management, CRM and ERP systems to enable extraction of performance information on operational and project information	Review and refine the performance measurement process and criteria. Perform a procurement selection process for the best fit institutional and employee performance management solution.

20 Compliance Requirements

ACTS/STDS	REQUIREMENTS	OUTPUT
ECT ACT 2002 SANS/ISO COBIT Framework SARS ACT PFMA 1999 SAICA Accounting Standards	- ERP Systems including e-Commerce Applications must have in-build systems controls (Prevention, Detection, and Corrective) and security logs and Audit trails for all executed transactions. <i>Ref ECT Act, SANS/ISO, COBIT Framework</i> - SARS requires that Tax obligations on electronic Transactions should be submitted online <i>Ref .SARS Act, PFMA Act, Accounting Std</i> - Authentication ,Encryptions and digital signatures ,Public Key Infrastructure e-Commerce processes) <i>Ref .ECT Act 2002 , COBIT, SANS/ISO</i>	- Develop a Business Rule Document for ERPs – incorporating all requirements - SLA- If Application architecture is outsourced, then incorporate compliance requirements in the Service Level Agreement(SLA)
Intellectual Property (IP) Act Copyright Act 2002 COBIT SANS/ISO	- General Project Management(Program Planning & Monitoring) - Budget Scheduling of IT Projects - Software cost estimation - Software Configuration Management - Critical Path Methodology(CPM) - Systems Development, tools and Productivity <i>Ref. IP Act</i> - Business Application Systems Development - Aids- CASE , 4GLs <i>Ref COBIT SANS/ISO</i>	- Develop Methodology for Development Architecture - Security Policy
ECT ACT 2002 TELECOM. Act SANS/ISO COBIT	- Application Controls - Application Services - Information Management - Communication services - System Services - Security Issues - Output Management - General Controls	- Develop Business Rules - Develop Security Policy

C. K.

ACTS/STDS	REQUIREMENTS	OUTPUT
COBIT / ICT Governance Framework SANS/ISO	▪ Computer room Operation Management ▪ Physical Site Management ▪ Physical & Logical Access Controls ▪ Protection of Data input/Processing & Output, Storage , Backups ▪ Archiving of information ▪ Change Control Management ▪ Disaster Recovery Planning ▪ Business Continuity Planning ▪ Training manuals ▪ Network/System Management ▪ Solution Availability ▪ Service Management ▪ Configuration Management Ref COBIT SANS/ISO	▪ ICT Governance Framework ▪ Develop Security Policy ▪ Develop DRP/BCP ▪ Develop a training and certification program
ECT Act 2002 Telecomm. Act SANS/ISO COBIT	▪ Hard ware Architecture (Mainframe Computers, Mini Computers, Micro Computers) ▪ Hard ware Acquisition, Hardware maintenance Program ▪ Hardware Monitoring Procedures ▪ Information Systems Network & Telecommunication Infrastructure : ○ Network Architecture Methods ○ Internet ○ Local Area Networks(LANs) ○ Wireless Networks ○ Wider Area Network(WANs) ○ Integrated Voice, Data & Video ▪ Telecommunications Monitoring Procedures ▪ Trans boarder Data flow ▪ Telecommunications Monitoring Procedure Ref. ECT Act, Telecom Act ,COBIT, SANS/ISO	▪ Develop ICT Infrastructure Policy
NARS Act 43 of 1996 Records Management	▪ Information Systems Network & Telecommunication Infrastructure : ○ Network Architecture Methods ○ Internet ○ Local Area Networks(LANs) ○ Wireless Networks ○ Wider Area Network(WANs) ○ Integrated Voice, Data & Video	▪ Integrated Records/Content management System

21 District Development Model as part of Enterprise Architecture

The district development model seeks to:

- Embody an approach by which the three spheres of government and state entities work in unison (jointly) with other development partners in an impact-oriented way and where there is higher performance and accountability for coherent service delivery and development outcomes;
- It influences spatialisation and reprioritisation of government planning, budgeting, implementation and reporting in relation to jointly agreed outcomes and commitments; and
- This is facilitated through and anchored around the 'One Plan', 'One Budget', 'One District'.

ICT plays a pivotal role in ensuring that there is planning collaboration is seamless between the district, local municipalities, province and national government.

Through the e-Council concept roots development within communities and brings government closer to the people

Through the former IGR the planning involves the following clusters whose inputs are also ICT driven:

- Social;
- Economic;
- Infrastructure;
- Governance and Institutional Development; and
- Justice, Crime Prevention and Security.

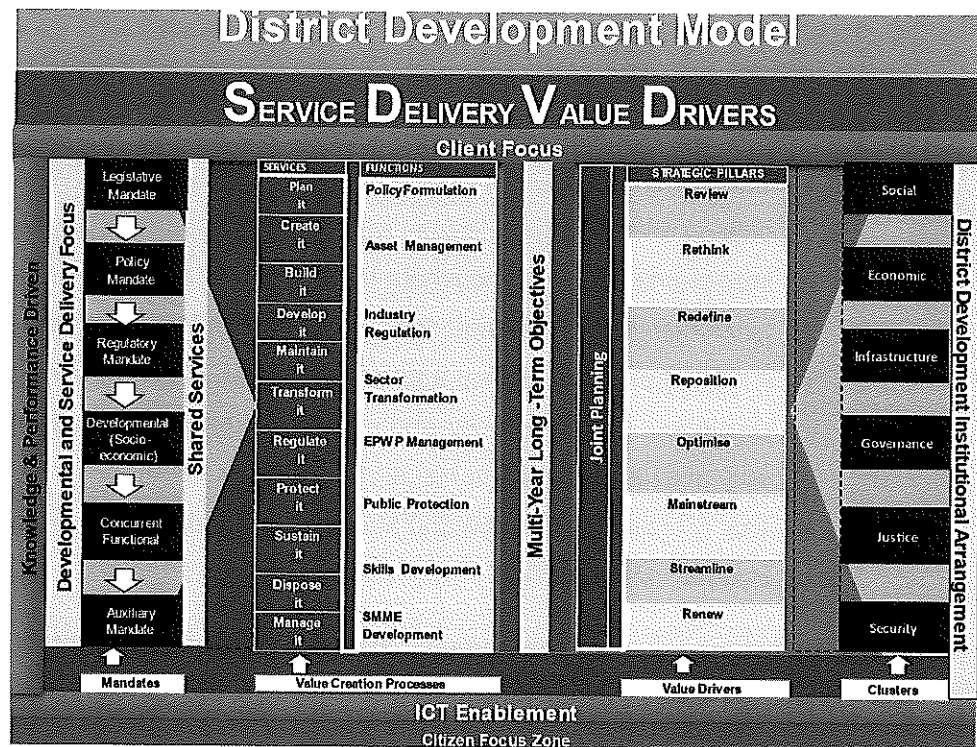


Figure 15: District Development Model

U.K.

Recommendations and Plan of Action

C, A

22 Recommendations

The ICT Strategy development process considered the roadmap in 19.7 above and the following recommendations as key to the success sustainable ICT investment which in turn will lead to the Business Continuity improvement. In this section summary action plans have been developed with estimated budgets.

- Elevation of the position of the driver of ICT in the organisation to a strategic Level
- PKSDM embarks on:
 - Aligning ICT with Business Strategy;
 - Developing ICT Governance Framework that will enable addressing of issues of business process improvements and business process integration;
 - Defining ICT Roles and Responsibilities;
 - Implementing a phased process-orientated approach; that seeks to deliver value through continuous improvement of business processes of the organisation;
 - Enforcing a process that will ensure a holistic and integrated decision-making process/framework for ICT investments;
 - Reviewing ICT Roadmap – Annually (recommendations/observations);
 - Reviewing ICT Strategy – recommendations/observations annually; and
 - Developing and implementing a Disaster Recovery (DRP) and Business Continuity (BCP) Plans.
 - Invest in a Backup Generator Set

22.1 Risk Management, Action Plans & Estimated Budgets

Below is the risk management, action plan and estimated budgets to enable the municipality to steer in the right direction.

V.L.

22.1.1 Risk Management

Strategic Objective	Risk	Risk Mitigation
Sound corporate governance through effective internal control environment	Loss of critical information forming portfolio of evidence	Establish Institutionalised electronic (interactive) records management system.
	ICT unable to function optimally	Prioritising the budget to fill critical vacancies and procurement of necessary ICT infrastructure.
	ICT Unit not governed as desired	Monitoring the implementation plan of ICT governance framework.
Provision of adequate strategic and technical support to achieve organizational goals	Undesired or unwarranted information and data loss	Development of institutional disaster recovery, backup and business continuity plan.
	Poor ICT Services to PKSDM Users	- Training and development on IT skills: and - Compliance with workplace skills plan.
	Untrained ICT resources managing data centre	Training and development to bridge skills gap.
	Council not able to continue with operations	Implement consistent reliable power backup strategy for data centre

C.R.

22.2 Plan of Action

Purpose: To create a "script" for operational improvement effort and support implementation.
Goal: Adherence to project initiatives, timelines and budget.
Results/Accomplishments: An outline of what should be achieved in the stated period using what resources.

Project Name What Will Be Done?	Action Steps What Must Be Done?	Accountable Who is the sponsor?	Responsibilities Who Will Do It?	Timeline By When? (Day/Month)	Resources A. Resources Available B. Resources Needed (financial, human, political & other)	Potential Barriers A. What individuals or organizations might resist? B. How?	Estimated Budget
Procurement of Generator Set	1. Draft Specifications 2. Benchmarking 3. Finalise specification 4. Procurement process 5. Appointment, preparation and signing of SLA 6. Implementation	SM: CS	ITO: ICT, SCM Officer, Disaster Management Officer Dep. CFO: SCM Contracts Management	End of July 2022	Human, Finance	None Budget availability Availability of equipment in the country	R450,000
Implementation of Help Desk	1. Present ICT Help desk solution to ICT Steering Committee, and to Management 2. Develop specifications 3. Initiate procurement process 4. Develop Marketing 5. Launch Help Desk Solution	ITO	ITO, MM, CFO	End of September 2022	Human, Finance	Time slot in EXCO to present the help desk solution	R300,000
Implement an interactive Electronic Council	1. System Planning – preliminary investigation report	ITO, MSS, SM:CS	ITO, MSS, SM:CS, SCM	November 2022	Human/Financial	Un-availability of support staff responsible for each committee for user requirements gathering of data	R150,000

Project Name What Will Be Done?	Action Steps What Must Be Done?	Accountable Who is the sponsor?	Responsibilities Who Will Do It?	Timeline By When? (Day/Month)	Resources A. Resources Available B. Resources Needed (financial, human, political & other)	Potential Barriers A. What individuals or organizations might resist? B. How?	Estimated Budget
Resolution tracking System	2. System analysis – User requirements specification 3. System design – Design functional Specification 4. System Implementation – Fully functional House resolution tracking system 5. Launch 6. Operation and Support						
Disaster Recovery Plan and Business Continuity Plan	1. Updated DRP 2. Project Plan with design architecture from SITA 3. Securing of dedicated line 4. Roll out of project 5. Procurement process	ITO: ICT	ITO: ICT Internal Audit SITA Project Manager SITA	August 2022	Human & Current DRP Human Finance & Human (SITA to assist with budget figure)	SITA internal processes	R2,500,000
Implementation Active Directory Service	1. Obtain licence 3. Procurement process 4. Implementation	ITO: ICT	ITO: ICT SCM Project Manager	July 2022	Finance & Human	None Timeframes Skills Finance	R100,000
Migrate to Microsoft 365	1. Order upgrade system 2. Upgrade system 3. Procurement process	ITO: ICT SITA Microsoft	ITO: ICT Business Units CFO, SCM	September 2022	Human & Finance		R450,000 Annually
Implement Business Intelligence System	1. Develop draft specifications 2. Request for Information (RFI)	ITO: ICT	ITO: ICT SCM	November 2022	Human & Finance	None Funding	TBA

C. R.

Project Name What Will Be Done?	Action Steps What Must Be Done?	Accountable Who is the sponsor?	Responsibilities Who Will Do It?	Timeline By When? (Day/Month)	Resources A. Resources Available B. Resources Needed (financial, human, political & other)	Potential Barriers What individuals or organizations might resist? A. B. How?	Estimated Budget
	3. Evaluation of RFI 4. Develop final specification 4. Procurement process 5. Appointment 6. Implementation 1. Draft service metrics for the various PKSDM business units 2. Workshop the service charter with business units 3. Implement service charter 1. Investigate Funding Model 2. Draw specifications 3. Procurement process 4. Appointment and SLA 5. Implementation	ITO: ICT Legal Services	ITO: ICT Business Units	August 2022	Human	- None - Business units delaying signing agreements	Nil
Implement a Service Charter - OLAs							
Implement an ERP Solution		ITO: ICT	ITO: ICT, HRM, Finance Secretary, contracts management Project Manager	July 2022	Human, Finance	- National Treasury buy-in - Availability of funds	TBA
Implement a digital signature solution	1. Draw specifications 2. Procure solution 3. Implement solution	ITO: ICT	MM: ITO: ICT CFO Project Manager	November 2022	Human, finance	- Availability of funds and procurement calendar - None	R250,000 (Annually) R120,000 (Once-off Implementation)
Implement an e-Council System	Issue of RFI Benchmarking Develop specifications Procurement process Implementation	ITO: ICT MSS: CS	ITO: ICT MSS: CS	Feb 2023	Human & Finance	- Availability of funds and procurement calendar - Implementation of Microsoft 365 and Microsoft SharePoint	R120,000
Investigate and implement a	1. Develop specifications	MSS: CS		Nov 2022	Finance Human	- None - Budget	R2 to R3 Million

Project Name What Will Be Done?	Action Steps What Must Be Done?	Accountable Who is the sponsor?	Responsibilities Who Will Do It?	Timeline By When? (Day/Month)	Resources A. Resources Available B. Resources Needed (financial, human, political & other)	Potential Barriers A. What individuals or organizations might resist? B. How?	Estimated Budget
Physical and Electronic Content Management Solution (ECM) SharePoint	2. Publish Terms of Reference 3. Procurement process 4. Appointment of service provider 5. Implementation of an Electronic Content Management System					Staff turnover	(This amount will be multi-year)
Establish ICT Lab for User Training on applications and technologies	1. Set up laboratory and buy equipment 2. Implement	ITO: ICT	ITO: ICT	September 2022	Finance, Human	None	Nil

U. A.

