



ICT GOVERNANCE FRAMEWORK



ICT GOVERNANCE FRAMEWORK

TABLE OF CONTENTS

GLOSSARY OF TERMS AND DEFINITIONS.....	3
EXECUTIVE SUMMARY	10
INTRODUCTION.....	11
PURPOSE OF THE FRAMEWORK	12
SECTION 1: GOVERNANCE OF ICT.....	13
1.1. GOVERNMENT SERVICE DELIVERY ENABLED THROUGH ICT	13
1.2. BENEFITS OF CORPORATE GOVERNANCE OF ICT	17
1.3. ADVANTAGES OF ADOPTING AN ICT GOVERNANCE FRAMEWORK	18
1.4. CHALLENGES OF ADOPTING AN ICT GOVERNANCE FRAMEWORK.....	19
1.5. CGICT AND GICT GOOD PRACTICE AND STANDARDS	20
1.6. LAYERED APPROACH TO CORPORATE GOVERNANCE OF ICT	21
1.7. CORPORATE GOVERNANCE IN UMKDM.....	22
1.8. CORPORATE GOVERNANCE OF ICT IN THE PUBLIC SERVICE	24
1.8.1. MEANS AND MECHANISMS:	Error! Bookmark not defined.
1.8.2. DECISION-MAKING AND MECHANISMS:	Error! Bookmark not defined.
1.8.3. ADOPTED STANDARDS.....	Error! Bookmark not defined.
1.9. OBJECTIVES OF THE CORPORATE GOVERNANCE OF ICT	26
1.10. PRINCIPLES FOR THE COPORATE GOVERNANCE OF ICT.....	26
1.11. MEARSURING, MONITORING AND BENCHMARKING	28
1.11.1. ICT GOVERNANCE MATURITY LEVELS.....	28
1.11.2. MEASURING AND MONITORING ACTIVITIES.....	28
1.11.3. ICT GOVERNANCE MEASUREMENTS.....	29



ICT GOVERNANCE FRAMEWORK

1.12.	SUPPORT FOR MUNICIPAL ICT GOVERNANCE	30
1.13.	GOVERNING LEGAL FRAMEWORK	31
SECTION 2: TACTICAL CONTEXT		32
	INTRODUCTION	32
2.1.	COBIT AS THE PROCESS FRAMEWORK FOR THE GOVERNANCE OF ICT	32
SECTION 3: IMPLEMENTATION APPROACH		34
3.1.	IMPLEMENTATION OF A GOVERNANCE OF ICT SYSTEM	34
ADDENDUM A – STANDARDS, CODES AND BEST PRACTICE		35
A1	GOVERNANCE	35
A.1.1.	KING III CODE GOVERNANCE	35
A.1.2	SANS 38500: 2008 ICT GOVERNANCE STANDARD	40
A.1.3.	COBIT GOVERNANCE FRAMEWORK	42
A2	SERVICE MANAGEMENT	46
A.2.1.	ITIL V2/3	46
A.2.2.	ISO/IEC 20000	49
A3	SECURITY MANAGEMENT	52
A3.1.	ISO/IEC 27001	52
A3.2.	ISO/IEC 27001 CONTROLS	54
A4	BUSINESS CONTINUITY / DISASTER RECOVERY	57
A4.1.	BS 25999	57
A4.2.	ISO/IEC 24762	59
A4.2.1.	ISO/IEC 2472 CONTROLS	61



ICT GOVERNANCE FRAMEWORK

GLOSSARY OF TERMS AND DEFINITIONS

Term	Definition
AG	Auditor-General
Accounting Officer	<p>Each municipal council is headed by a municipal manager who is the head of administration and also the accounting officer. The municipal manager advises council and its committees on administrative matters such as policy issues, financial matters, organisational requirements, and personnel matters.</p> <ul style="list-style-type: none"> • As accounting officer, the municipal manager is comparable to a director-general in the public service. • He/she has to personally provide reasons to council for the way in which the financial affairs of the departments of council had been conducted.
BCM	Business Continuity Management
BITA	Business IT Alignment
Business Goals	Statements that describe what the business will accomplish, or the business value a project will achieve - A clear vision of what you want to achieve; and how
Charter	Control Objectives for Information and Related Technology. An IT governance



ICT GOVERNANCE FRAMEWORK

	framework and toolset that allows managers to bridge the gap between control requirements, technical issues and business risks
CFO	Chief Financial Officer
CIO	Chief Information Officer
Control	A procedure or policy that provides a reasonable assurance that the information technology (IT) used by an organisation operates as intended
Corporate Governance	The set of responsibilities and practices exercised by the Council and executive management with the goals of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly
Deliverable	A term used in project management to describe a tangible or intangible object produced as a result of the project that is intended to be delivered to a customer
DRP	Disaster Recovery Planning
DPSA	Department of Public Service and Administration
EXCO	Executive Management
Executive Authority	Executive Authority means Executing



ICT GOVERNANCE FRAMEWORK

	<p>Authority</p> <ul style="list-style-type: none"> • In a Constitutional Institution: The Chairperson of the Constitutional Institution in relation to a Constitutional Institution with a body of persons, and in relation to a Constitutional Institution with a single office bearer, the incumbent of that office; • According to section 11(1) of the Municipal Systems Act (Act No. 32 of 2000) the executive and legislative authority of a municipality is exercised by the council of the municipality.
<p>Executive Management</p>	<p>Executive Management could include the Municipal Manager and the section 57 management. This normally constitutes the Executive Committee of the municipality.</p> <ul style="list-style-type: none"> • Each municipal council is headed by a municipal manager who is the head of administration and also the accounting officer. The municipal manager advises council and its committees on administrative matters such as policy issues, financial matters, organisational requirements, and personnel matters. • As accounting officer, the municipal manager is comparable to a director-general in the public service. • He/she has to personally provide reasons to council for the way in which the financial affairs of the departments of



ICT GOVERNANCE FRAMEWORK

	council had been conducted.
Framework	A basic conceptual structure with items which supports a particular approach to a specific objective. E.g. CobiT is an IT governance framework
GICT	Governance of ICT
Governance of ICT	<p>The effective and efficient management of IT resources to facilitate the achievement of company strategic objectives. (King III: 2009)</p> <p>Is the responsibility of executives and the board of directors and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategy and objectives (ITGI 2005)</p>
Governance Principles	The vehicle to translate the desired behavior into practical guidance for day-to-day management
ICT	Information and Communication Technology also referred to as IT
ISACA®	Information Systems Audit and Control Association
ISMS	Information Security Management System



ICT GOVERNANCE FRAMEWORK

IT Goals	Processes that ensure that IT sustains and extends the organisation's strategy and objectives
IT	Information Technology
ITIL	IT Infrastructure Library
ISO/IEC	International Standards Organisation (ISO) and the International Electro Technical Commission (IEC)
ISO/IEC 20000	The first international standard for IT service management. It was developed in 2005, by ISO/IEC JTC1 SC7 and revised in 2011
ISO/IEC 24762	International standard - Security techniques - Guidelines for information and communications technology disaster recovery services
ISO /IEC 27001/2	Part of the ISO/IEC 27000 family of standards, is an Information Security Management System (ISMS) standard published in October 2005
ISO 38500	Corporate governance of information technology standard. Provides a framework for effective governance of IT to assist those at the highest level of organisations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organisations' use of IT
JSE	Johannesburg Stock Exchange



ICT GOVERNANCE FRAMEWORK

JTC1/SC27	Joint Technical Committee 1 / Sub Committee 27 (ISO/IEC Technical Committee with responsibility for IT standards)
KGI	Key Goal Indicator. A KGI is a measure of "what" has to be accomplished
King III	The King Code of Corporate Governance for South Africa 2009
KPI	Key Performance Indicator. While KGI's focus on "what", the KPI's are concerned with "how"
LG Seta	Local Government Sector Training Authority
LGTS	Local Government Turnaround Strategy
Metrics	A measure of an organisation's activities and performance
MFMA	Municipal Finance Management Act
NT	National Treasury
OGC	Office of Government Commerce (UK Government Department, custodian of ITIL)
Policy	A principle or rule to guide decisions and achieve rational outcome(s)
PAIA	Promotion of Access to Information Act
Process	Sequence of interdependent and linked procedures which, at every stage, consume



ICT GOVERNANCE FRAMEWORK

	one or more resources
Procedure	A fixed, step-by-step sequence of activities or course of action (with definite start and end points) that must be followed in the same order
Responsible	Refers to the person who must ensure that activities are completed successfully
Risk	The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).
SABS	South African Bureau of Standards
SANS	System Administration, Network and Security Institute. SANS is by far the largest source for information security training and security certification in the world
SCOA	Standard Charter of Accounts
Strategy	The direction and scope of an organisation over the long-term: which achieves advantage for the organisation through its configuration of resources



ICT GOVERNANCE FRAMEWORK

EXECUTIVE SUMMARY

Government transformation is, at a strategic level, informed by government-wide key priority areas that have been translated into 12 strategic outcomes, guided by the Batho Pele principles of equal access to services, increased productivity and lowering of costs. The purpose of information and communication technology (ICT) is to enable the Umkhanyakude District Municipality (UMKDM) in its quest for service delivery. The ICT House of Value depicts the values and key focus areas of ICT service delivery. These strategic outcomes, principles, values and key focus areas inform the acquisition, management and use of ICT.

To determine whether ICT in Government delivers an enabling service, various investigations have been done to establish the shortcomings of ICT service delivery. The first of these was the 1998 Presidential Review Commission (PRC) report, which stated that all-important ICT-decisions should come from the senior political and managerial leadership of the state and not be delegated to the technology specialists, and further that the management of ICT should be on the same level as the management of other resources. It furthermore advocated a common enabling framework of governance.

Since the publication of the PRC report, little has changed with respect to the governance of ICT in the Public Service. This was confirmed by the Auditor General's (AG) information systems review of governance of ICT in government conducted in 2008/09 and again in 2009/10. The AG recommendations included the following:

- a) A government-wide Governance of ICT Framework should be put in place to implement a national ICT strategy to address ICT risks based on defined processes and standards; and
- b) The Governance of ICT roles responsibilities should be defined and implemented to ensure adequate government ICT enablement

The view that ICT should be governed and managed at a Political Leadership and



ICT GOVERNANCE FRAMEWORK

Executive Management level is supported by international accepted good practice and standards in the form of King III Code of Good Governance, ISO 38500 Standard for the Corporate Governance of ICT and COBIT a comprehensive Governance ICT Process Framework. It also places accountability for governance of ICT fully in the hands of Political Leadership and Executive Management.

This accountability enables UMKDM to align the delivery of ICT services with the UMKDM's strategic goals.

The executive authority and management of UMKDM need to extend corporate governance as a good management practice to ICT (Corporate Governance of ICT). In the execution of the Corporate Governance of ICT, they should provide the necessary strategies, architectures, plans, frameworks, policies, structures, procedures, processes, mechanisms and controls, and ethical culture. To strengthen the Corporate Governance of ICT further, the IT Manager should be an integral part of the Executive Management of the UMKDM.

INTRODUCTION

- (a) The scope of the Framework applies to all national and provincial institutions as defined by the Public Service Act of 1994 as amended (Schedules 1 to 3). However, the local governments (municipalities) are not listed or mentioned in Schedule 1 - lastly updated on 02/04/2012, Schedule 2 - lastly updated on 19/10/2012, and Schedule 3 - lastly updated on 11/05/2012.
- (b) The Framework recognises that Institutions are diverse. It is thus not possible to produce a blueprint applicable to all Institutions.
- (c) National and provincial institutions that have a supervisory role over institutions and entities that do not fall under this Act may prescribe a GICTF for such entities, which should be aligned with this Framework.
- (d) The Municipal Guide / Roadmap to Successful ICT Governance, should be seen as complimentary to the DPSA Framework as it builds on to the concepts, standards, codes and best practice that is listed in the DPSA Framework.



ICT GOVERNANCE FRAMEWORK

PURPOSE OF THE FRAMEWORK

The purpose of this Framework is to institutionalise the Corporate Governance of and Governance of ICT as an integral part of corporate governance within Umkhanyakude District Municipality (UMKDM) in a uniform and coordinated manner.

The Framework provides a set of principles and practices with which UMKDM must comply.

The Corporate Governance of ICT is a continuous function that should be embedded in all operations of UMKDM, from Executive Authority and Executive Management level to the business and ICT service delivery.

Corporate Governance of ICT is implemented in two different layers:

- a) Corporate Governance of ICT (this CGICTPF); and
- b) Governance of ICT (GICTF).

To enable a UMKDM to implement this CGICTPF, a three-phase approach will be followed:

- (a) **Phase 1:** Corporate Governance environment will be established in UMKDM
- (b) **Phase 2:** UMKDM will plan and implement business and ICT strategic alignment; and
- (c) **Phase 3:** UMKDM will enter into an iterative process to achieve continuous improvement of Corporate Governance of and Governance of ICT.

This Framework has been developed in line with the South African Local Government Association's (SALGA) ICT Governance Guidelines and the Department of Public Service Administration's Corporate Governance of ICT Framework (CGICTF)

The SALGA ICT Governance Guidelines is complimentary to the DPSA Framework as it builds on to the concepts, standards, codes and best practice that is listed in the DPSA Framework. While the DPSA Framework is strategically positioned, the Guideline, although also strategic in nature, is more tactically and operationally focused. The Guideline will be used as a reference when implementing the Framework. It should be considered as moving from "strategic intent" (the DPSA Framework) to "operational excellence".



SECTION 1: GOVERNANCE OF ICT

1.1.GOVERNMENT SERVICE DELIVERY ENABLED THROUGH ICT

In support of the achievement of the 12 strategic outcomes, the government has adopted certain ICT values and key focus areas to be achieved as contained in the ICT House of Value shown below.

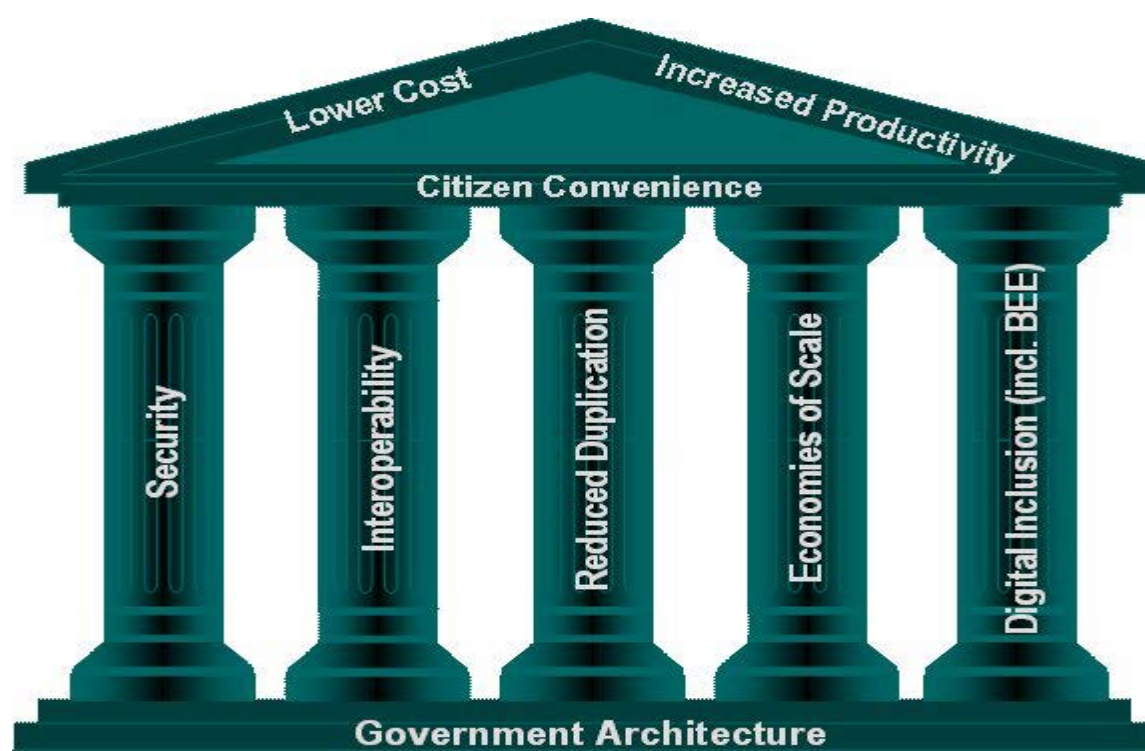


Figure 1: ICT House of Value



ICT GOVERNANCE FRAMEWORK

Strategic outcome	Related strategic goals in ICT House of Value		Values
	Primary Influencing goals	Secondary Influencing goals	
Outcome 1: Basic Education	Government Architecture Interoperability Digital inclusion Economies of scale Reduced duplication	Security	Lower cost Citizen convenience Increased productivity
Outcome 2: A long and healthy life for all South Africans	Government Architecture Security Interoperability Reduced duplication Digital inclusion	Economies of scale	Lower cost Citizen convenience Increased productivity
Outcome 3: All people in SA are and feel safe	Government Architecture Security Digital inclusion	Interoperability Reduced duplication Economies of scale	Lower cost Citizen convenience Increased productivity
Outcome 4: Decent	Interoperability	Government	Lower cost



ICT GOVERNANCE FRAMEWORK

employment through inclusive economic growth	Digital inclusion Economies of scale Reduced duplication Security	Architecture	Citizen convenience Increased productivity
	Primary Influencing goals	Secondary Influencing goals	
Outcome 5: Skills and capable workforce to support an inclusive growth path	Government Architecture Interoperability Digital inclusion	Economies of scale Security Reduced duplication	Lower cost Citizen convenience Increased productivity
Outcome 6: An efficient, competitive and responsive economic infrastructure network	Government Architecture Interoperability Digital inclusion Economies of scale Security Reduced duplication		Lower cost Citizen convenience Increased productivity
Outcome 7: Vibrant, equitable, sustainable rural communities contributing towards	Government Architecture Digital inclusion Security	Reduced duplication Economies of scale	Lower cost Citizen convenience Increased



ICT GOVERNANCE FRAMEWORK

food security for all			productivity
Outcome 8: Sustainable human settlement and improved quality household life	Government Architecture Digital inclusion	Interoperability Economies of scale Security Reduced duplication	Lower cost Citizen convenience Increased productivity
Outcome 9: Responsive, accountable, effective and efficient local government system	Government Architecture Interoperability Digital inclusion Economies of scale Security Reduced duplication		Lower cost Citizen convenience Increased Productivity
Outcome 10: Protect and enhance our environmental assets and natural resources	Government Architecture Economies of scale Reduced duplication	Interoperability Security Digital inclusion	Lower cost Citizen convenience Increased Productivity
Outcome 11: Create a better SA, a better Africa and a better world	Government Architecture Security	Interoperability Economies of scale Reduced duplication	Lower cost Citizen convenience Increased



ICT GOVERNANCE FRAMEWORK

	Digital inclusion		Productivity
Outcome 12: An efficient, effective and development-oriented Public Service and empowered, fair and inclusive citizenship	Economies of scale Security Reduced duplication		

Table 1: Strategic Outcome 12, “An efficient, effective and development-oriented Public Service and empowered, fair and inclusive citizenship”, is the main driver of ICT business enablement in the Public Service.

1.2.BENEFITS OF CORPORATE GOVERNANCE OF ICT

When the Corporate Governance of ICT in UMKDM is effectively implemented and maintained, the following benefits are realised:

- Improved achievement of Public Service-wide and UMKDM strategic goals;
- Improved effective public service delivery through ICT-enabled access to government information and services;
- Improved ICT enablement of business;
- Improved delivery of ICT service quality;
- Improved stakeholder communication;
- Continuous improvement of business and ICT alignment;
- Improved trust between ICT, the business and citizens;
- Lower costs;
- Increased alignment of investment towards strategic goals;
- Improved return on ICT-enabled investment;



ICT GOVERNANCE FRAMEWORK

- (k) ICT risks managed in line with the priorities and appetite of the Public Service and the UMKDM;
- (l) Appropriate security measures to protect the UMKDM and employee information;
- (m) Improved management of business-related ICT projects;
- (n) Improved management of information as it is managed on the same level as other resources such as people, finance and material in the Public Service;
- (o) ICT pro-actively recognises opportunities and guides UMKDM and the Public Service in timeous adoption of appropriate technology;
- (p) Improved ICT ability to learn and agility to adapt to changing circumstances; and
- (q) ICT executed in line with legislative and regulatory requirements.

1.3.ADVANTAGES OF ADOPTING AN ICT GOVERNANCE FRAMEWORK

ICT has become an integral part of doing business today, as it is fundamental to the support, sustainability and growth of UMKDM. ICT cuts across all aspects, components and processes in business and is therefore not only an operational enabler for UMKDM, but an important strategic asset which can be leveraged to create opportunities and to gain competitive advantage.

As well as being a strategic asset to UMKDM, ICT also presents UMKDM with significant risks. The strategic asset of ICT and its related risks and constraints should be well governed and controlled to ensure that ICT supports the strategic objectives of the organisation.

By adopting an ICT Governance Framework, Mayor and Municipal Manager are in compliance with King III Code of Governance which stipulates that prudent and reasonable steps must be taken with respect to ICT governance.

Adopting a strategic approach to ICT Governance extends the horizon of thinking beyond the boundary of “are we compliant, yes or no?” towards performance management, guiding optimal allocation of a municipality’s finite resources and providing the means to capture value back from the investment.



ICT GOVERNANCE FRAMEWORK

1.4. CHALLENGES OF ADOPTING AN ICT GOVERNANCE FRAMEWORK

One of the major challenge in implementing an ICT Governance Framework stems from the difficult task of taking a strategic viewpoint to assess and improve governance. The decision to go ahead has to come from the highest office. If the major benefits of an ICT Governance Framework are not realised at this level, implementation attempts are most certainly doomed.

Successful adoption requires orientation, education, and training which does not happen overnight. The availability of suitably skilled staff to perform the many different tasks associated with a framework implementation comes with its own challenges. Training staff in the various required disciplines are often expensive and is time consuming.

One size does not fit all. Although there is an abundance of guidance available, these still has to be tailored to municipal specific requirements. The ability to improve governance is intrinsically tied to the ability to effectively measure it, the tacit knowledge of employees and successfully navigating the complex jungle of best practice, regulations, legislation, standards and the strategic intent of management.

For ICT governance to be successful, it should be a workable solution able to deal with the challenges and pitfalls presented by ICT. It should not only prevent problems but also enable competitive advantage. ICT risks are closely related to business risks, because ICT is the enabler for most business strategies. The management and control of ICT should therefore, be a shared responsibility between the business and the ICT functions, with the full support and direction of executive management. ICT governance provides the oversight and monitoring of these activities within a wider enterprise governance scheme.

1.5.CGICT AND GICT GOOD PRACTICE AND STANDARDS

In recognition of the importance of the Governance of ICT, a number of internationally recognised frameworks and standards, such as King III Code, ISO/IEC 38500 and COBIT have been developed to provide context for the institutionalisation of the Corporate Governance of ICT.

- (a) **The King III Code:** The most commonly accepted Corporate Governance Framework in South Africa is also valid for the UMKDM. It was used to inform the Corporate Governance of ICT principles and practices in this framework and to establish the relationship between Corporate Governance of and Governance of ICT.
- (b) **ISO/IEC 385007:** Internationally accepted as the standard for Corporate Governance of ICT; it provides governance principles and a model.
- (c) **COBIT:** An internationally accepted process framework for implementing Governance of ICT. COBIT fully supports the principles of the King III Code and the ISO/IEC 38500 standard in the Corporate Governance of ICT.

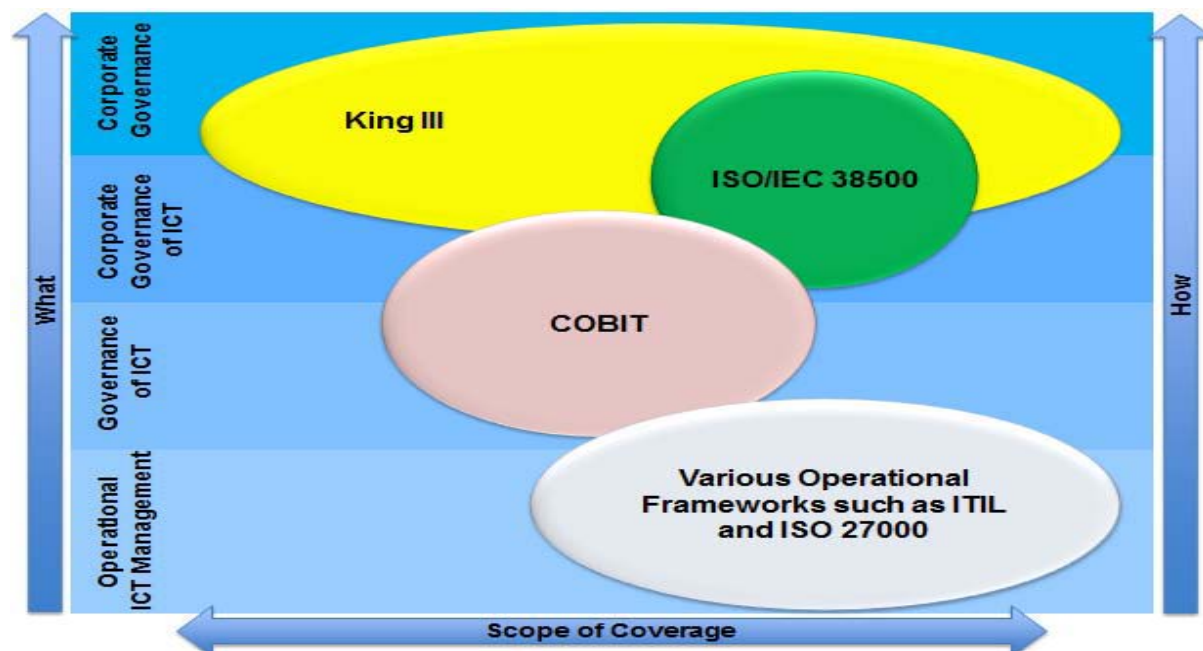


Figure 2: Interrelationship of different Frameworks and Standards



ICT GOVERNANCE FRAMEWORK

1.6.LAYERED APPROACH TO CORPORATE GOVERNANCE OF ICT

Corporate Governance of ICT encompasses two levels of decision-making, authority and accountability to satisfy the expectations of all stakeholders:

- (a) Facilitating the achievement of UMKDM's strategic goals (Corporate Governance of ICT); and
- (b) The efficient and effective management of ICT service delivery (Governance of ICT)

The implementation of Corporate Governance of ICT UMKDM thus consists of the following layered approach:

- (a) This CGICTPF, which addresses the Corporate Governance of ICT layer.
- (b) COBIT, this will be adapted and implemented as the GICTF on the Governance of ICT layer.

Figure 3: demonstrates the different governance layers with their related frameworks and standards.

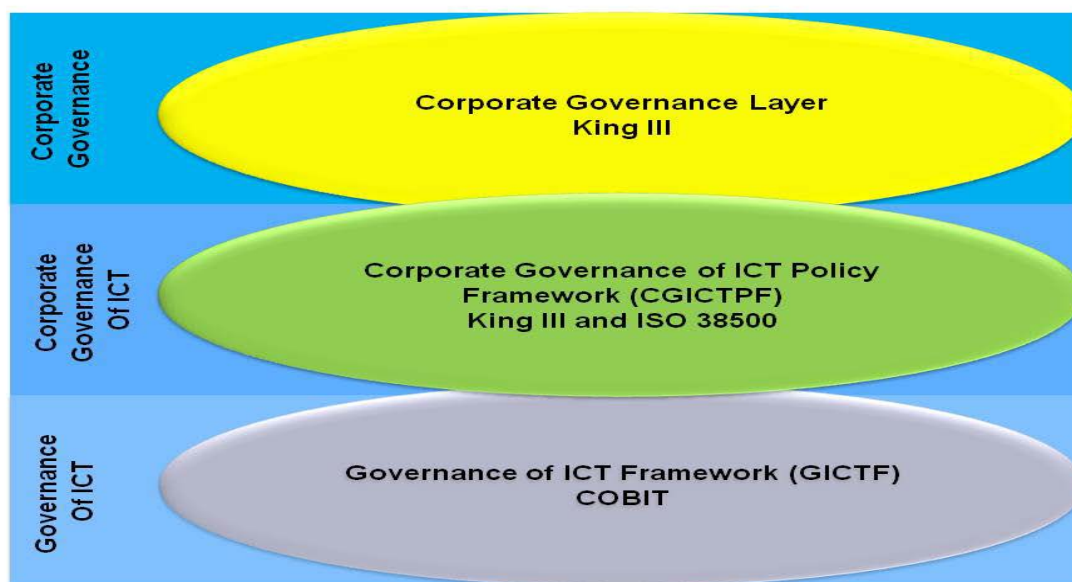


Figure 3: Governance Layers



1.7. CORPORATE GOVERNANCE IN UMKDM

The purpose of corporate governance is to create value for UMKDM's stakeholders. It consists of a governance system that affects the way UMKDM is managed and controlled. It also defines the relationships between stakeholders, the strategic goals of UMKDM.

Corporate governance is a vehicle through which value is created within UMKDM departmental context. Value creation means realising benefits while optimising resources and risks. This value creation takes place within a governance system that is established by this Policy Framework.

A governance system refers to all the means and mechanisms that enable the Accounting Officer and Executive Management of UMKDM to have a structured and organised say in:

- (a) **Evaluating** internal and external context, strategic direction and risk to conceptualise the UMKDM's strategic goals and how it will be measured;
- (b) **Directing** the UMKDM in the execution of the strategic goals to ensure that value is realised and risk is managed; and
- (c) **Monitoring** the execution of the strategic goals within UMKDM against the measures identified for attaining the strategic goals.

Corporate governance is also concerned with individual accountability and responsibilities within UMKDM. It describes how the UMKDM is directed and controlled and is in particular concerned with:

- (a) **Organisation** - the organisational structures, and coordinating mechanisms (such as steering forums) established within UMKDM and in partnership with external bodies;
- (b) **Management** – the individual roles and responsibilities established to manage business change and operational services; and
- (c) **Policies** - the frameworks established for making decisions and the context and constraints within which decisions are taken.

Figure 4 depicts how the governance system functions. The executive leadership, which is accountable, provides the strategic direction of the department. The strategic direction, together with the external and internal context, determines the strategic goals. Corporate Governance of and the Governance of ICT are executed at Executive Management level



ICT GOVERNANCE FRAMEWORK

through the function of evaluation, direction and monitoring. The management of business execution is done through the organisational structure and utilisation of the relevant resources.



Figure 4: Corporate Governance System

The strategic direction, together with the external and internal context, influences the strategic goals. Corporate Governance and the Corporate Governance of ICT are executed on Executive Management level through the function of evaluation, direction and monitoring. The management of business execution is done through the organisational structure and utilisation of the relevant resources.

The executive leadership and management of UMKDM are accountable and responsible to implement a governance system.



1.8.CORPORATE GOVERNANCE OF ICT IN UMKDM

CobIT the Control Framework is aimed at delivering IT Value while minimising IT Risk. The IT Resources as mentioned in the IT Charter need to be managed by a structured set of IT Processes. CobIT provides a complete list of 34 IT Processes that can be used to verify the completeness of activities and responsibilities: however, they need not all apply; even more they can be combined as required by each organisation.

1.8.1. PLAN AND ORGANISE(PO):

- a. **PO3- Determine Technological Direction.** - The Information service function determines the technology direction to support the business. There needs to be a plan that encompasses aspects such as systems architecture, technological direction, acquisition plans, standards and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems and investments.
- b. **PO6- Communicate Management Aims and Direction.** – Implement an on-going communication programme to articulate the mission, service objectives, policies and procedures, approved and supported by management. The communication ensures awareness and understanding of business and IT risks, objectives and direction.

1.8.2. ACQUIRE AND IMPLEMENT(AI):

- a. **AI4 –Enable Operation and Use.** - Knowledge about systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure proper use and operation of applications.
- b. **AI5 – Procure IT Resources.** – This requires the definition and enforcement of procurement procedures and setup of contractual arrangements and the acquisition itself

1.8.3. DELIVER AND SUPPORT(DS):

- a. **DS1- Define and Manage Service Levels.** – Effective communication between IT management and business customers regarding services required is enabled by a documented definition of an agreement on IT services and service levels. This



ICT GOVERNANCE FRAMEWORK

process enables alignment between IT services and the related business requirements.

- b. **DS2 – Manage Third Party Services.** – The need to assure that services by third parties (suppliers, vendors etc) meet business requirements requires an effective third party management process.
- c. **DS8 – Manage Service Desk and Incidents.** – Timely and effectively response to IT user queries and problems requires a suitably designed and efficiently executed service desk and incident management process.

1.8.4. MONITOR AND EVALUATE(ME):

- a. **ME4- Provide IT Governance.** – Establish an effective IT governance framework, include defining organisational structures, processes, leadership, roles and responsibilities to ensure that IT investments are aligned and delivered in accordance with the municipality's strategies and objectives.

1.8.5. ADOPTED STANDARDS FOR UMKDM

UMKDM elects to adapt and/or adopt the following standards and frameworks:

- (a) DPSA Corporate Governance Of ICT Policy Framework;
- (b) ICT Security (e.g. ISO/IEC 27000 set);
- (c) Service Management (e.g. ITIL); CobIT Framework
- (d) Interoperability Standards (e.g. MIOS);



ICT GOVERNANCE FRAMEWORK

1.9.OBJECTIVES OF THE CORPORATE GOVERNANCE OF ICT

- Identify, establish and prescribe a uniform Governance of ICT Framework (GICTF) and implementation guideline for the Public Service;
- Embed the Corporate Governance of and Governance of ICT as a subset of Corporate Governance;
- Create business value through ICT enablement by ensuring business and ICT strategic alignment;
- Provide relevant ICT resources, organisational structure, capacity and capability to enable ICT service delivery;
- Achieve and monitor ICT service delivery performance and conformance to relevant internal and external policies, frameworks, laws, regulations, standards and practices;
- Implement the governance of ICT in the UMKDM based on the COBIT process framework
- Position the IT Manager function as an integral part of Executive Management

1.10. PRINCIPLES FOR THE COPORATE GOVERNANCE OF ICT

PRINCIPLE	DESCRIPTION
Principle 1: Political Mandate	<ul style="list-style-type: none"> The Corporate Governance of ICT must enable the municipality's political mandate The Executive Authority must ensure that the Corporate Governance of ICT achieves the political mandate of the municipality.
Principle 2: Strategic Mandate	<ul style="list-style-type: none"> The Corporate Governance of ICT must enable the municipality's strategic mandate The Accounting Officer must ensure that the Corporate Governance of ICT assists in achieving the municipality's strategic plans.
Principle 3: Corporate Governance of ICT	<ul style="list-style-type: none"> The Accounting Officer is responsible for the Corporate Governance of ICT. The Accounting Officer must create an enabling



ICT GOVERNANCE FRAMEWORK

	environment in respect of the Corporate Governance of ICT within the applicable legislative and regulatory landscape and information security context.
Principle 4: ICT Strategic Alignment	<ul style="list-style-type: none"> ICT service delivery must be aligned with the strategic goals of the municipality. The Executive Management must ensure that ICT service delivery is aligned with the municipality's strategic goals and that the municipality accounts for current and future capabilities of ICT. It must ensure that ICT is fit for purpose at the current service levels and quality for both current and future municipal needs.
Principle 5: Significant ICT Expenditure	<ul style="list-style-type: none"> The Executive Management must monitor and evaluate significant ICT expenditure. Executive Management must monitor and evaluate major ICT expenditure, ensure that the ICT expenditure is made for valid municipal business enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed.
Principle 6: Risk Management and Assurance	<ul style="list-style-type: none"> Executive Management must ensure that ICT risks are managed and that then ICT function is audited. Executive Management must ensure that ICT risks are managed within the municipal risk management practice. It must also ensure that the ICT function is audited as part of the municipal audit plan.



ICT GOVERNANCE FRAMEWORK

Principle 7: Organisational Behavior	<ul style="list-style-type: none"> Executive Management must ensure that ICT service delivery is sensitive to organizational behavior / culture. Executive Management must ensure that the use of ICT demonstrates the understanding of and respect for the organisational behaviour / culture.
--------------------------------------	---

Table 2: The principles for the Corporate Governance of ICT and their descriptions.

1.11. MEASURING, MONITORING AND BENCHMARKING

1.11.1. ICT GOVERNANCE MATURITY LEVELS

The King III Code defines a wide range of requirements that need to be fulfilled by all organisations (also Local Government) in South Africa, including an awareness of levels of maturity in the governance of ICT. Levels of maturity are recognised using the criteria of assigned responsibility to fulfil the King III principles and practices, the activities executed in support of the principles and practices, the supporting documents in place and the nature of performance measurements being monitored.

1.11.2. MEASURING AND MONITORING ACTIVITIES

It's not about doing things right, it is about doing the RIGHT things right. How does this relate to Governance?

Typically decisions have to be made on a continual basis on how to allocate and reallocate resources and how to prioritise ICT activities and plans. Information on the importance of all current projects and ICT processes and how they are performing as an integral part of the overall ICT strategy is required on an on-going basis. Are they on track to reach business benefits? Does it require improvement, what are the business risks, how well are risks managed?

Amongst the many definitions for ICT governance, it can also be defined as:



ICT GOVERNANCE FRAMEWORK

“A framework that consists of the leadership, organisational structures and processes that ensure that the organisation’s ICT sustains and extends the organisation’s strategies and objectives.”

This translates into several responsibilities and activities areas:

- (a) Business-IT strategic alignment, so that current ICT operations support the business and future ICT organisation enable the business;
- (b) ICT value delivery, identify and perform those ICT activities that actually deliver value to the business;
- (c) Risk management, that must become an integral part of all ICT processes so that risks are identified and be dealt with;
- (d) Performance measurement, to monitor if goals are reached and provide directions for improvement where deviations are observed.

1.11.3. ICT GOVERNANCE MEASUREMENTS

The measurement of ICT Governance at UMKDM shall be taken over a medium to long term. It consists of a number of steps as follows:

- (a) Definition phase - ICT Governance goals or Key Goal Indicators (KGI's) need to be established at the top organisational level (Municipal Manager's Office). These goals are then cascade down in the municipal ICT organisation. A KGI is a measure of "what" has to be accomplished.
- (b) Translation phase - A cascading (breakdown) of the KGI into measurable (weighing factor) Key Performance Indicators (KPI's) and sources/processes cross the municipal divisions. A KPI define and measure progress toward organisational goals. While KGI's focus on “what”, the KPI's are concerned with “how”
- (c) Measurement phase - Audits/assessments (self-assessments) are conducted across the ICT environment on relevance of Governance activities/plans/processes /RACI within the



ICT GOVERNANCE FRAMEWORK

business value chain. The level of accomplished ICT Governance process roll-out per business requirement is measured

- (d) Management phase - From the audit/assessment results, the cascaded KPI/KGI are analysed for shortfalls and potential business risks coming from these (where not predefined) to enable corrective actions.
- (e) Opportunity phase - Performance measures are then compared against the goals and the goals are checked for validity. Goal may be redefined because of business dynamics. Adjustments are budgeted for and implemented and where necessary KGI/KPIs are adjusted and the cycle starts over, periodically.

1.12. SUPPORT FOR MUNICIPAL ICT GOVERNANCE

SALGA: By establishing the Corporate Governance of ICT Guideline to enable successful adoption and implementation of the Corporate Governance of ICT Framework Policy.

CoGTA: By monitoring and influencing improvements to address system deficiencies and duplication at municipalities

National Treasury: Support in the assessment of IT control environments and assist with the implementation of IT controls

DPSA: In consultation with the GITO council, extended the IT governance framework policy developed for national and provincial departments to incorporate local government.

Office of the Premier: By extending the approved GITO to incorporate support to municipalities and monitoring of the implementation thereof.

The Auditor-General conducts audits, and reports on its findings regarding the Corporate Governance of and Governance of ICT to the relevant authorities.



ICT GOVERNANCE FRAMEWORK

1.13. GOVERNING LEGAL FRAMEWORK

UMKDM, and by extension IT Department, operates within the ambits of the South African legal and the regulatory framework. The following Acts and Regulatory Codes must be observed and complied with as part of IT Governance:

- (a) Electronic Communications Act,
- (b) National Archives And Records Service Of South Africa Act,
- (c) Electronic Communications And Transactions Act,
- (d) Electronic Communications Security Act,
- (e) Independent Communications Authority of South Africa Act,
- (f) Regulation of Interception of Communications and Provision of Communication-related
- (g) Information Act,
- (h) Promotion of Access to Information Act,
- (i) State Information Technology Agency Act,
- (j) Technology Innovation Agency Act,
- (k) Telecommunications Act,
- (l) MFMA,



SECTION 2: TACTICAL CONTEXT

INTRODUCTION

This CGICTPF will direct the implementation of the Governance of ICT, which will be based on COBIT.

The implementation of COBIT will establish a common knowledge and reference base for Monitoring and Evaluation (M&E).

2.1. COBIT AS THE PROCESS FRAMEWORK FOR THE GOVERNANCE OF ICT

COBIT shall enable UMKDM to achieve its strategic goals by deriving optimal value from ICT through the realisation of benefits and optimising resources and risk.

COBIT is not a standard – it is a process framework within which UMKDM has flexibility regarding implementation, according to its specific environmental context.

As a set of Governance of ICT and management processes, COBIT provides managers, ICT users and auditors with the following:

- (a) Standard indicators;
- (b) Processes for implementing the Governance of ICT;
- (c) Good practice to maximise the corporate value in using ICT.
- (d) Identification of the accountability and responsibilities of business and ICT
- (e) process owners;
- (f) Metrics to measure the achievement of the ICT-related goals; and
- (g) A model to measure governance of ICT process maturity.

Principle 1 of the five COBIT principles provides an “Integrator Framework” to ensure seamless integration with other relevant standards and frameworks such as ITIL (Service Management), CMMI / ISO/IEC 15504 (Maturity Assessments) and ISO/IEC 2700x (Security).



ICT GOVERNANCE FRAMEWORK

Principle 4, Governance Enablers, provides for the implementation of a governance and management system for corporate ICT. There are seven categories of enablers:

- (a) Processes;
- (b) Principles and policies;
- (c) Organisational structures;
- (d) Skills and competences;
- (e) Culture and behaviour;
- (f) Service capabilities;
- (g) Information.



ICT GOVERNANCE FRAMEWORK

SECTION 3: IMPLEMENTATION APPROACH

3.1.IMPLEMENTATION OF A GOVERNANCE OF ICT SYSTEM

Corporate Governance of ICT incorporates two layers of decision-making, authority and accountability to satisfy the expectations of all stakeholders by:

- (a) Facilitating the achievement of a department's strategic goals (Corporate Governance of ICT layer); and
- (b) The efficient and effective management of ICT service delivery (Governance of ICT layer).

To enable UMKDM to implement both this Policy Framework and COBIT, implementation will be done in 3 phases:

- (a) **Phase 1:** The creation of an enabling CGICT and Governance of ICT (GICT) environments which involves the development and implementation of a CGICT and GICT Policy depicting delegations, roles and responsibilities and organisational structure.
- (b) **Phase 2:** Strategic alignment in which Political and Strategic leadership provides strategic direction for enablement of the business by ICT and the governance and management of ICT by the GITO; and
- (c) **Phase 3:** Continuous improvement of CGICT is achieved through on-going monitoring, evaluation and directing.



ADDENDUM A – STANDARDS, CODES AND BEST PRACTICE

A1 GOVERNANCE

A.1.1. KING III CODE GOVERNANCE

The King Code on Governance for South Africa ("King III") was launched on 1 September 2009. It came into effect and replaced the then existing King II Code on Corporate Governance ("King II") on 1 March 2010.

King III sets out a number of key governance principles which should be read together with best practice recommendations on how to carry out each principle. A number of Practice Notes have also been issued by the Institute of Directors to assist entities in implementing King III.

King III's principles and recommendations must be seen against the legislative requirements contained in the 2008 Act and the Public Finance Management Act of 1999. This is reflected in the terminology used in King III with "must" indicating a legal requirement and "should" indicating where application of King III will result in good governance.

Significantly, King III also applies to all entities incorporated in and resident in SA irrespective of their manner or form of incorporation or establishment. The application of King III is also mandatory for JSE listed companies.

In a change of approach, King III moves from a "comply or explain" approach to an "apply or explain" approach. The "apply and explain" approach requires a greater consideration of how a principle or a recommended practice in King III could be applied. A board may conclude that applying a recommended practice is not necessarily in the best interests of the company and apply a different practice provided that it explains the practice adopted and its reasons for doing so.

At a high level, the King III Code of Governance addresses the following governance components:

- (a) Ethical leadership and corporate citizenship
- (b) Boards and directors



ICT GOVERNANCE FRAMEWORK

- (c) Audit committees
- (d) The governance of risk
- (e) The governance of information technology
- (f) Compliance with laws, rules, codes and standards
- (g) Internal audit
- (h) Governing stakeholder relationships
- (i) Integrated reporting and disclosure

In addition, the King Committee also commissioned a number of Practice Notes to assist with the insight into and practical application of King III. Practice Notes are aimed at providing high-level guidance to those individuals charged with governance to enable them to execute those duties and are not intended to serve as detailed implementation guides.

The table below summarises chapter 5 of the code. Chapter 5 focus specifically on

ICT:

Table 4: KING III Section

Principles		Recommended Practice	
King III Section	Principle	Sub section	Practice
		5.1.1	The board should assume the responsibility for the governance of IT and place it on the board agenda
		5.1.2	The board should ensure that an IT charter and policies are established and implemented.



ICT GOVERNANCE FRAMEWORK

5.1	The board should be responsible for information technology (IT) governance	5.1.3	The board should ensure promotion of an ethical IT governance culture and awareness and of a common IT language.
		5.1.4	The board should ensure that an IT internal control framework is adopted and implemented
		5.1.5	The board should receive independent assurance on the effectiveness of the IT internal controls
5.2	IT should be aligned with the performance and sustainability objectives of the company	5.2.1	The board should ensure that the IT strategy is integrated with the company's strategic and business processes
		5.2.3	The board should ensure that there is a process in place to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT
5.3	The board should delegate to management the responsibility for	5.3.1	Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework



ICT GOVERNANCE FRAMEWORK

	the implementation of an IT governance framework	5.3.2	The board may appoint an IT steering committee of similar function to assist with its governance of IT
		5.3.3	The CEO should appoint a Chief Information Officer responsible for the management of IT
5.4	significant IT investments and expenditure	5.4.2	The board should ensure that intellectual property contained in information systems are protected
		5.4.3	The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services
5.5	IT should form an integral part of the company's risk management	5.5.1	Management should regularly demonstrate to the board that the company has adequate business resilience arrangements in place for disaster recovery
		5.5.2	The board should ensure that the company complies with IT laws and that IT related rules, codes and standards are considered
		5.6.1	The board should ensure that there are systems in place for the management of information which should include information



ICT GOVERNANCE FRAMEWORK

5.6	The board should ensure that information assets are managed effectively		security, information management and information privacy
		5.6.2	The board should ensure that all personal information is treated by the company as an important business asset and is identified
		5.6.3	The board should ensure that an Information Security Management System is developed and implemented
		5.6.4	The board should approve the information security strategy and delegate and empower management to implement the strategy
5.7	A risk committee and audit committee should assist the board in carrying out its IT responsibilities	5.7.1	The risk committee should ensure that IT risks are adequately addressed
		5.7.2	The risk committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks
		5.7.3	The audit committee should consider IT as it relates to financial reporting and the going concern of the company
		5.7.4	The audit committee should consider the use of technology to improve audit coverage and



ICT GOVERNANCE FRAMEWORK

efficiency

A.1.2 SANS 38500: 2008 ICT GOVERNANCE STANDARD

The ISO\IEC 38500 standard on the Corporate Governance of ICT was published by

International Standards Organisation (ISO) and the International Electro Technical

Commission (IEC) in June 2008. The standard originated from an Australian standard AS 8015.

This standard provides a framework for effective governance of ICT, to assist those at the highest level of organisations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organisations' use of ICT. This standard was adopted and published by South African Standards Bureau in July 2009 and is available from the SABS.

The standard was published by the SABS for the South African environment in July

2009 and included the following as part of its national forward:

“SANS 38500:2008 provides guidance on the effective and efficient use of corporate governance of information technology (IT) operations within organisations.

Organisations that subscribe to SANS 38500:2008 as an international guideline to construct its corporate governance of ICT environment, should note that efficient and effective corporate governance of ICT is derived from the interpretation, implementation and execution of the guidelines of SANS 38500:2008 in an organisational environment.

Adherence to SANS 38500:2008 guidelines assures stakeholders the confidence in the effective corporate governance of IT in the organisation. This assurance is not absolute and depends on how the guidelines of SANS 38500:2008 are interpreted, implemented and executed in order to govern the corporate use of IT effective and efficiently.

SANS 38500:2008 should be implemented in conjunction with South African legislation and regulations. SANS 38500:2008 compliments and dovetails with de facto corporate



ICT GOVERNANCE FRAMEWORK

governance codes of practices such as the KING II and KING III reports on corporate governance for South Africa.

Definitions within SANS 38500:2008 were developed in order to cater for a global audience. Local definitions of terms can therefore, where relevant, be adopted in order to align the standard with the South African environment.

SANS 38500:2800 is a principle based standard, so when the governing body adopt these principles it should provide the fundamental reference that influences their behaviour when governing the use of ICT. The standard offers the following six principles:

SANS 38500:2008 – Principles	Description
Principle 1: Responsibility	This responsibility principle states that individuals or groups will be granted the required authority to accept and dispose of their responsibilities in the use of IT. Although not explicitly stated, the governing body may delegated certain responsibilities, but remain accountable for the outcome
Principle 2: Strategy	This strategy principle states that the business strategy considers the capabilities of IT (both current and future) and that IT strategic plans enables the on-going realisation of the business' strategic intent
Principle 3: Acquisition	This acquisition principle states that IT is procured through sound and transparent investment decisions; that these decisions will consider the appropriate balance between risk and reward; and



ICT GOVERNANCE FRAMEWORK

	that investment benefits/outcomes are tracked to realisation
Principle 4: Performance	This performance principle states that the organisation should deliver fit for purpose, quality IT services, at the required service levels that will contribute to the organisation delivering on its strategic intent
Principle 5: Conformance	This conformance principle states that the organisation in the use of IT, continually complies with all applicable legislation and regulation by embedding it in their policies and practices
Principle 6: Human behaviour	This human behaviour principle states that the organisation should respect the needs of people in the use IT by embedding it in their policies and practices

Table 5: Six principles of SANS 38500:2800

A.1.3. COBIT GOVERNANCE FRAMEWORK



ICT GOVERNANCE FRAMEWORK

Control Objectives for Information and related Technology (CobiT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. CobiT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution.

For ICT to be successful in delivering against business requirements, management should put an internal control system or framework in place. The CobiT control framework contributes to these needs by:

- Making a link to the business requirements
- Organising ICT activities into a generally accepted process model
- Identifying the major ICT resources to be leveraged
- Defining the management control objectives to be considered

The business orientation of CobiT consists of linking business goals to ICT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and ICT process owners

The process focus of CobiT is illustrated by a process model that subdivides ICT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of ICT. Enterprise architecture concepts help identifies the resources essential for process success, i.e., applications, information, infrastructure and people.

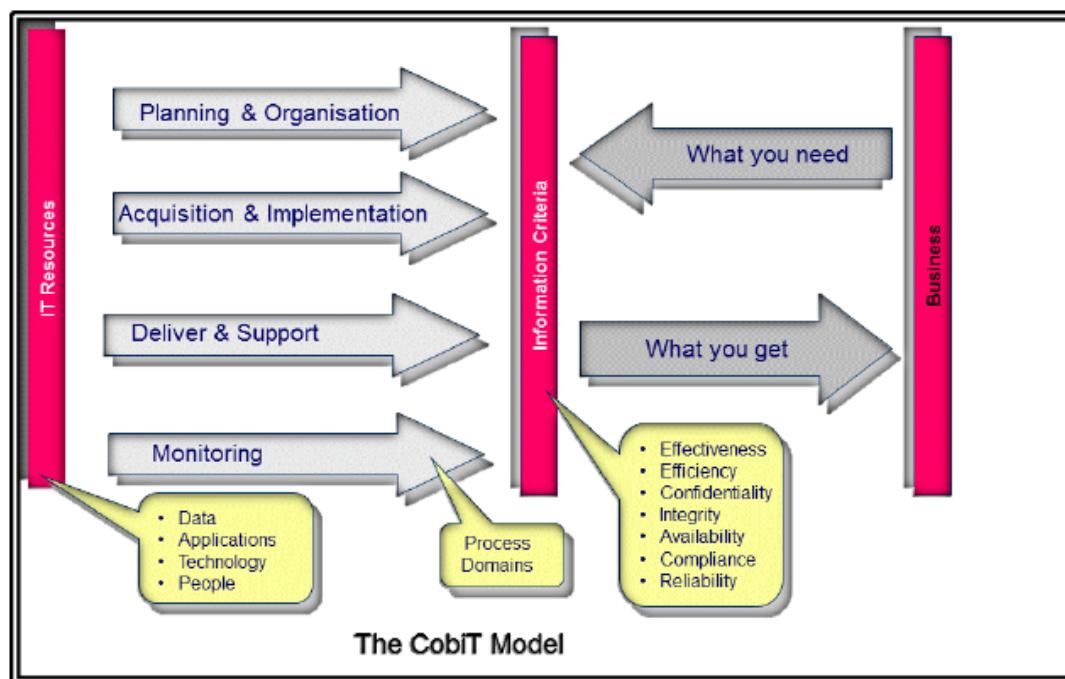


Figure5: COBIT Model

CobiT ICT Governance focus areas can be summarised as follows:

Strategic alignment focuses on ensuring the linkage of business and ICT plans; defining, maintaining and validating the ICT value proposition; and aligning IT operations with enterprise operations.

- Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that ICT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of ICT.
- Resource management is about the optimal investment in, and the proper management of, critical ICT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure. Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.



ICT GOVERNANCE FRAMEWORK

- Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.



ICT GOVERNANCE FRAMEWORK

A2 SERVICE MANAGEMENT

A.2.1. ITIL V2/3

ITIL was developed by the Office of Government Commerce (OGC) within the UK Treasury Department in the late 1980s to improve the efficiency and effectiveness of government procurement. Today, OGC uses ITIL to create centers of excellence in program management to serve as examples of best practices across government.

The common terminology and consistent service levels and processes presented by ITIL are particularly valuable to companies looking to standardise their best practices across business units and geographical locations. Incorporating ITIL into IT service management is one way to assure customers that they'll receive a consistent quality of service and efficiency, whether they're dealing with operations in different geographical locations.






	Service Strategy	Continual Service Improvement	Service Design	Service Transition	Service Operation
ITIL Service Component					
ITIL Processes	<ul style="list-style-type: none"> Financial Management Demand Management Service Portfolio Management Strategy Generation Supplier Management 	<ul style="list-style-type: none"> 7 Step Improvement Service Reporting Service Measurement Service Level Management 	<ul style="list-style-type: none"> Service Catalogue Management Service Level Management Availability Management Capacity Management Service Continuity Management Information Security Management 	<ul style="list-style-type: none"> Transition Planning & Support Change Management Service Asset & Configuration Management Release & Deployment management Service Validation & Testing Evaluation Knowledge Management 	<ul style="list-style-type: none"> Event management Incident Management Request Fulfilment Problem Management Accessmanagement Operational Activities Change Management Configuration Management Release & Deployment Management Capacity Management Knowledge Management Financial Management for IT Services IT Service Continuity Management

Figure7: ITIL V2/3



ICT GOVERNANCE FRAMEWORK

Although the current version is version3, all the core processes of version 2 have been retained, albeit in a different category. ITIL version 2 defined service management best practices as 10 core processes divided into two major functional areas: Service Support and Service Delivery. Within each of the 10 core areas is a series of activities designed to help ICT not only manage and maintain current demands for service, but also react quickly to change as the nature of ICT dependency evolves.

Service Support is all about delivering the ICT services customers need to stay up and running. This includes fixing the root cause of problems to prevent repetition of incidents and ensure that any modifications don't introduce new problems. ITIL identifies five key components of service support:

- Incident management focuses on restoring service to the customer as quickly as possible to the agreed-upon service levels
- Problem management explores the root cause of an incident and focuses on determining a solution or solutions that will eliminate it from the ICT infrastructure
- Change management deals with maintaining control over the ICT infrastructure to prevent changes from creating new incidents
- Configuration management links ICT assets to their relationships, both physical and in respect to key business processes, so that management can make intelligent decisions about service priorities
- Release management addresses how to introduce new hardware and software into an organization as smoothly as possible without creating new incidents and problems.

Service Delivery is all about making sure that ICT has everything in its environment to deliver support on a day-to-day basis to the agreed-upon service levels the customer demands. This includes sufficient people on the service desk, sufficient capacity, enough lines, equipment, software, and so on. ITIL identifies five key components of service delivery:

- Service-level management emphasizes the importance of determining service needs from the customer inward, not from ICT outward. First, define the customer's service needs and then build a service-level agreement around those needs.



ICT GOVERNANCE FRAMEWORK

- Financial management focuses on understanding exactly what it costs to supply a particular service to a customer. It involves thinking of ICT as a business rather than just an internal department.
- Capacity management looks at managing both the capacity of assets and the performance of those assets to provide the level of service the customer needs.
- Availability management is all about providing service to the customer – to agreed service levels -- as well as continually examining the reliability of the ICT infrastructure to improve upon the availability of service.
- Continuity management identifies the critical services a business needs to stay in business and focuses on providing the right level of service to maintain continuity during typical day-to-day operations as well as under adverse circumstances such as disaster recovery.

With the publication of version 3, a number of additional components as listed below have been added:

- Strategy generation
- Service design aspects
- Supplier management
- Outsourced models
- Service knowledge management system
- Application design and management
- Technology architecture design and management
- Service measurement
- Event measurement
- Request fulfilment

The list below shows how Service Delivery and Service Support have been positioned in version 3:



ICT GOVERNANCE FRAMEWORK


ITIL V2	ITIL V3	
Change Management	Service Transition	
Configuration Management	Service Transition	
Incident Management	Service Operation	
Problem Management	Service Operation	
Release Management	Service Transition	
Service Desk	Service Operation	
Availability Management	Service Design	
Capacity Management	Service Design	
Financial Management	Service Strategy	
IT Continuity Management	Service Design	
Service Level Management	Continual Service Improvement	

Figure8: Service Delivery and Service Support in ITIL V3

A.2.2. ISO/IEC 20000

ISO/IEC 20000-1:2005 defines the requirements for a service provider to deliver managed services.



ICT GOVERNANCE FRAMEWORK

It may be used:

- By businesses that are going out to tender for their services;
- To provide a consistent approach by all service providers in a supply chain;
- To benchmark ICT service management;
- As the basis for an independent assessment;
- To demonstrate the ability to meet customer requirements;
- To improve services.

ISO/IEC 20000-1:2005 promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and customer requirements.

For an organisation to function effectively it has to identify and manage numerous linked activities. Co-ordinate integration and implementation of the service management processes provides the ongoing control, greater efficiency and opportunities for continual improvement.

Organisations require increasingly advanced facilities (at minimum cost) to meet their business needs. With the increasing dependencies in support services and the diverse range of technologies available, service providers can struggle to maintain high levels of customer service. Working reactively, they spend too little time planning, training, reviewing, investigating, and working with customers. The result is a failure to adopt structured, proactive working practices. Those same service providers are being asked for improved quality, lower costs, greater flexibility, and faster response to customers.

In contrast, effective service management delivers high levels of customer service and customer satisfaction. It also recognizes that services and service management are essential to helping organizations generate revenue and be cost-effective. The ISO/IEC 20000 series enables service providers to understand how to enhance the quality of service delivered to their customers, both internal and external.



ICT GOVERNANCE FRAMEWORK

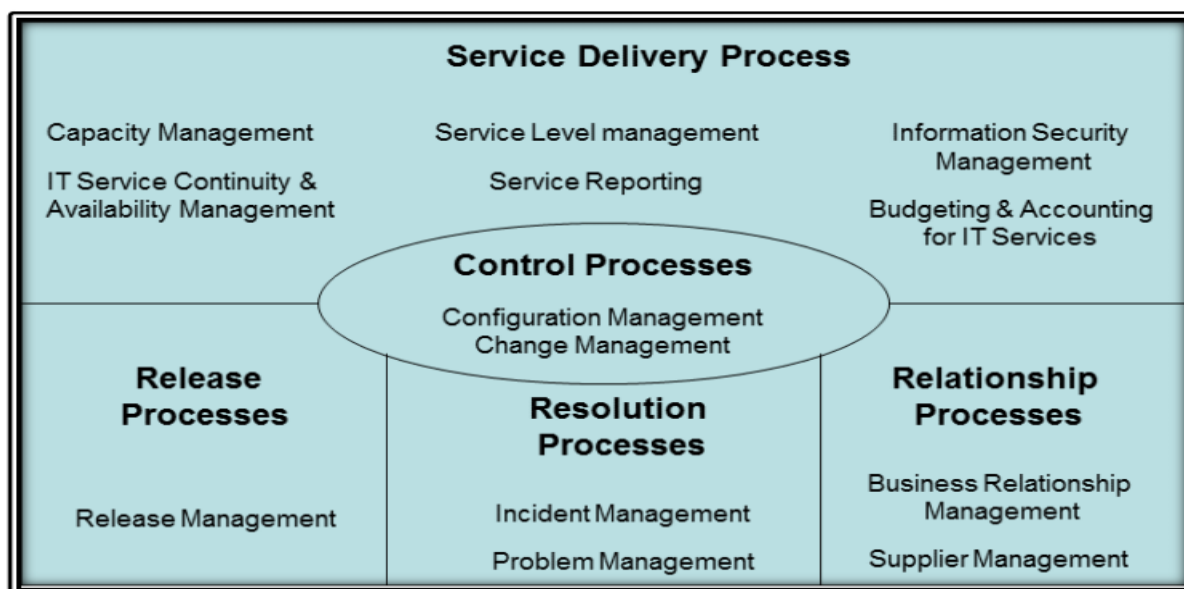


Figure9: ISO/IEC 20000 service delivery process

The ISO/IEC 20000 series draws a distinction between the best practices of processes, which are independent of organisational form or size and organisational names and structures. The ISO/IEC 20000 series applies to both large and small service providers, and the requirements for best practice service management processes are independent of the service provider's organisational form. These service management processes deliver the best possible service to meet a customer's business needs within agreed resource levels, i.e. service that is professional, cost-effective and with risks which are understood and managed



A3 SECURITY MANAGEMENT

A3.1. SO/IEC 27001

ISO/IEC 27001 is the formal standard against which organisations may seek independent certification of their Information Security Management Systems (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organisations).

The standard covers all types of organisations (e.g. commercial enterprises, government agencies and non-profit organisations). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the organisation's overall risk management processes. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

ISO/IEC 27001 provides an ISMS model for adequate and proportionate security controls to protect information assets and give confidence to interested parties.

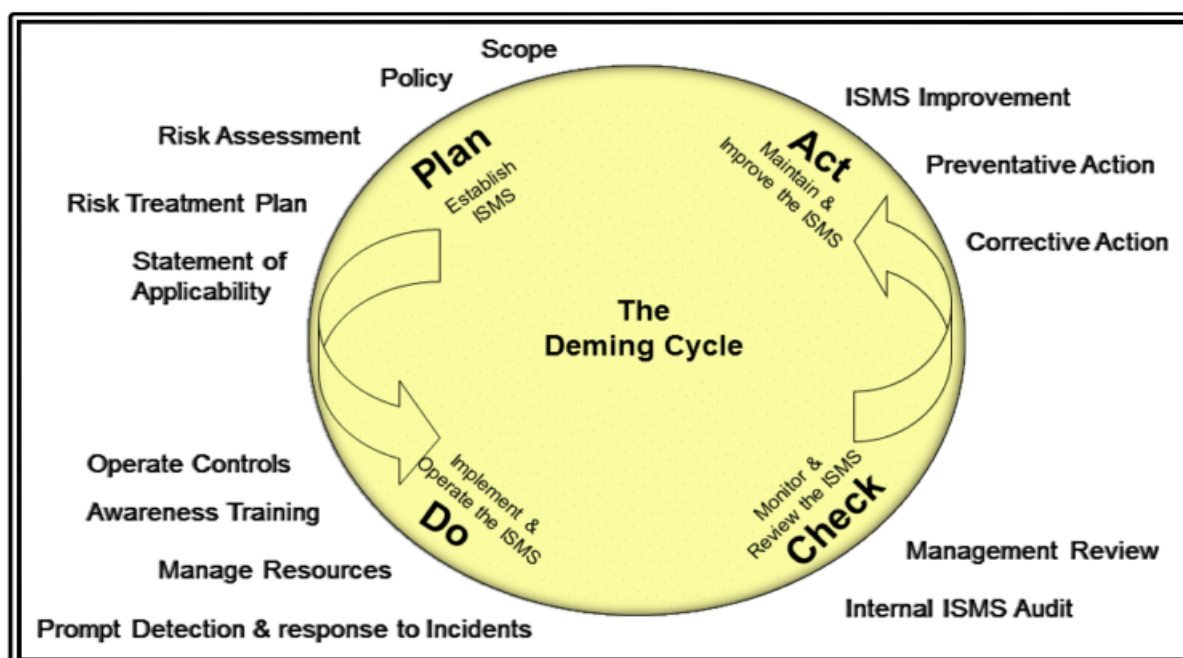


Figure10: SMS model for adequate and proportionate security controls



ICT GOVERNANCE FRAMEWORK

According to JTC1/SC27, the ISO/IEC committee responsible for the '27000 series and related standards, '27001 "is intended to be suitable for several different types of use, including:

- (a) Use within organisations to formulate security requirements and objectives;
- (b) Use within organisations as a way to ensure that security risks are cost-effectively managed;
- (c) Use within organisations to ensure compliance with laws and regulations;
- (d) Use within an organisation as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organisation are met;
- (e) The definition of new information security management processes;
- (f) Identification and clarification of existing information security management processes;
- (g) Use by the management of organisations to determine the status of information security management activities;
- (h) Use by the internal and external auditors of organisations to demonstrate the information security policies, directives and standards adopted by an organisation and determine the degree of compliance with those policies, directives and standards;
- (i) Use by organisations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organisations that they interact with for operational or commercial reasons;
- (j) Implementation of a business enabling information security; and
- (k) Use by organisations to provide relevant information about information security to customers."

The information security controls from ISO/IEC 27002 are noted in an appendix to ISO/IEC 27001, rather like a menu. Organisations adopting ISO/IEC 27001 are free to choose whichever specific information security controls are applicable to their particular information security situations, drawing on those listed in the menu and potentially supplementing them with other a la carte options. As with ISO/IEC 27002, the key to selecting applicable controls is to undertake a comprehensive assessment of the organisation's information security risks.



ICT GOVERNANCE FRAMEWORK

A3.2. ISO/IEC 27001 CONTROLS

ISO/IEC 27002 Controls		
Clause	Sec	Control Objective
Organisation of Information security	6.1	Internal Organisation
	6.2	External Parties
Asset Management	7.1	Responsibility for Assets
	7.2	Information classification
Human Resource Security	8.1	Prior to Employment
	8.2	During Employment
	8.3	Termination or change of employment
Physical and Environmental Security	9.1	Secure Areas
	9.2	Equipment security
Communications and Operations Management	10.1	Operational Procedures and responsibilities
	10.2	Third Party Service Delivery Management
	10.3	System Planning and Acceptance
	10.4	Protection against Malicious and Mobile Code
	10.5	Back-Up
Communications and Operations Management	10.6	Network Security Management
	10.7	Media Handling



ICT GOVERNANCE FRAMEWORK

	10.8	Exchange of Information
	10.9	Electronic Commerce Services
	10.10	Monitoring
Access Control	11.1	Business Requirement for Access Control
	11.2	User Access Management
	11.3	User Responsibilities
	11.4	Network Access control
	11.5	Operating System Access Control
	11.6	Application access control
	11.7	Mobile Computing and Teleworking
Information Systems Acquisition Development and Maintenance	12.1	Security Requirements of Information Systems
	12.2	Correct Processing in Applications
	12.3	Cryptographic controls
	12.4	Security of System Files
	12.5	Security in Development & Support Processes
	12.6	Technical Vulnerability Management
Technical Vulnerability Management	13.1	Reporting Information Security Events and Weaknesses
	13.2	Management of Information Security



ICT GOVERNANCE FRAMEWORK

		Incidents and Improvements
Business Continuity Management	14.1	Information Security Aspects of Business Continuity Management
Compliance	15.1	Compliance with Legal Requirements
	15.2	Compliance with Security Policies and Standards and Technical compliance
	15.3	Information System Audit Considerations

Table 6: ISO/IEC 27001 Controls



A4 BUSINESS CONTINUITY / DISASTER RECOVERY

A4.1. BS 25999

Continued operations in the event of a disruption whether due to a major disaster or a minor incident, are a fundamental requirement for any organisation. BS 25999, the world's first British standard for business continuity management (BCM), has been developed to help you minimize the risk of such disruptions.

By helping to put the fundamentals of a BCM system in place, the standard is designed to keep a company's business going during the most challenging and unexpected circumstances – protecting its staff, preserving its reputation and providing the ability to continue to operate and trade.

BS 25999 has been developed by a broad based group of world class experts representing a cross-section of industry sectors and the government to establish the process, principles and terminology of Business Continuity Management.

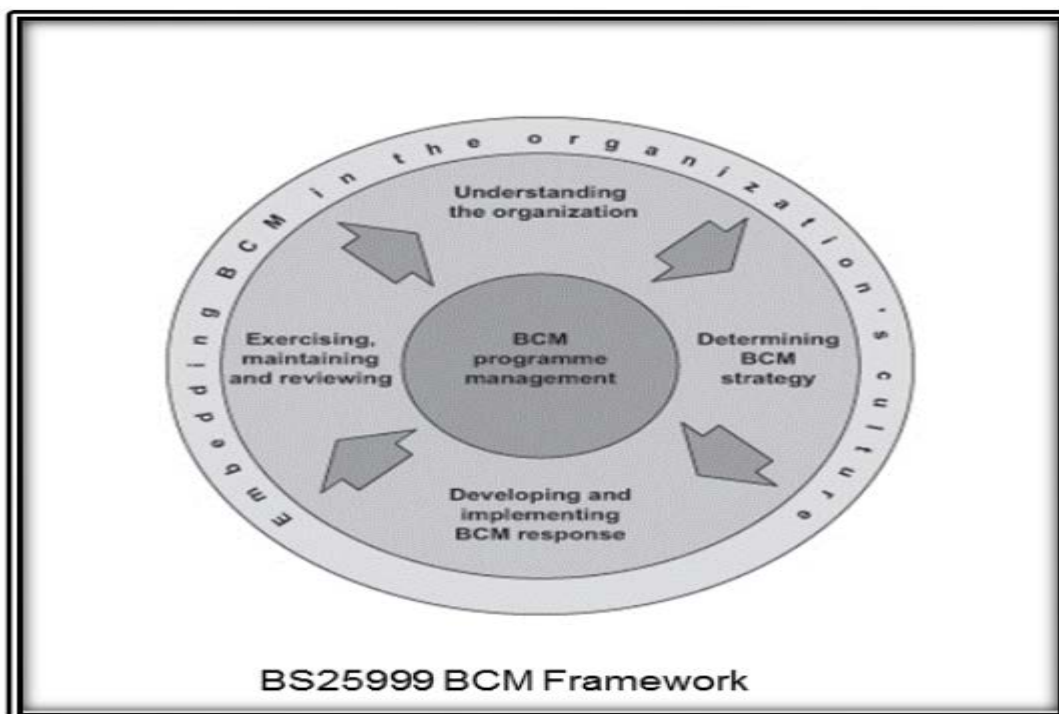


Figure11: BS 25999 framework



ICT GOVERNANCE FRAMEWORK

BS 25999 comprises two parts:

BS 25999-1:2006 Part 1, the Code of Practice, provides BCM best practice recommendations. Please note that this is a guidance document only.

- (a) Section 1 - Scope and Applicability: This section defines the scope of the standard, making clear that it describes generic best practice that should be tailored to the organisation implementing it
- (b) Section 2 - Terms and Definitions: This section describes the terminology and definitions used within the body of the standard
- (c) Section 3 - Overview of Business Continuity Management: A short overview is the subject of the standard. It is not meant to be a beginner's guide but describes the overall processes, its relationship with risk management and reasons for an organization to implement along with the benefits
- (d) Section 4 - The Business Continuity Management Policy: Central to the implementation of business continuity is having a clear, unambiguous and appropriately resourced policy
- (e) Section 5 - BCM Program Management: Program management is at the heart of the whole BCM process and the standard defines an approach
- (f) Section 6 - Understanding the organisation: In order to apply appropriate business continuity strategies and tactics the organization has to be fully understood, its critical activities, resources, duties, obligations, threats, risks and overall risk appetite.
- (g) Section 7 - Determining BCM Strategies: Once the organisation is thoroughly understood the overall business continuity strategies can be defined that are appropriate.
- (h) Section 8 - Developing and implementing a BCM response: The tactical means by which business continuity is delivered. These include incident management structures, incident management and business continuity plans.
- (i) Section 9 - Exercising, maintenance, audit and self-assessment of the BCM culture:
- (j) Without testing the BCM response an organization cannot be certain that they will meet their requirements. Exercise, maintenance and review processes will enable then business continuity capability to continue to meet the organizations goals.
- (k) Section 10 - Embedding BCM into the organizations culture: Business continuity should not exist in a vacuum but become part of the way that the organization is managed.

The contents of the Specification (BS 25999-2) are as follows:



ICT GOVERNANCE FRAMEWORK

- (a) Section 1 – Scope: Defines the scope of the standard, the requirements for implementing and operating a documented business continuity management system (BCMS)
- (b) Section 2 - Terms and Definitions: This section describes the terminology and definitions used within the body of the standard
- (c) Section 3 - Planning the Business Continuity Management System (PLAN): Part 2 of the standard is predicated on the well-established Plan-Do-Check-Act model of continuous improvement. The first step is to plan the BCMS, establishing and embedding it within the organisation.
- (d) Section 4 - Implementing and Operating the BCMS (DO): Actually implement ones plans. This section includes a number of topics that are found in Part 1 although Part 1 should only be used for general guidance and information. Only what is in Part 2 can be assessed.
- (e) Section 5 - Monitoring and Reviewing the BCMS (CHECK): To ensure that the BCMS is continually monitored the Check stage covers internal audit and management review of the BCMS
- (f) Section 6 Maintaining and Improving the BCMS (ACT): To ensure that the BCMS is both maintained and improved on an ongoing basis this section looks at preventative and corrective action.

A4.2. ISO/IEC 24762



ICT GOVERNANCE FRAMEWORK

ISO/IEC 24762 is aimed at aiding the operation of an Information Security Management System (ISMS) by providing guidance on the provision of Information and Communications Technology Disaster Recovery (ICT DR) services as part of business continuity management.

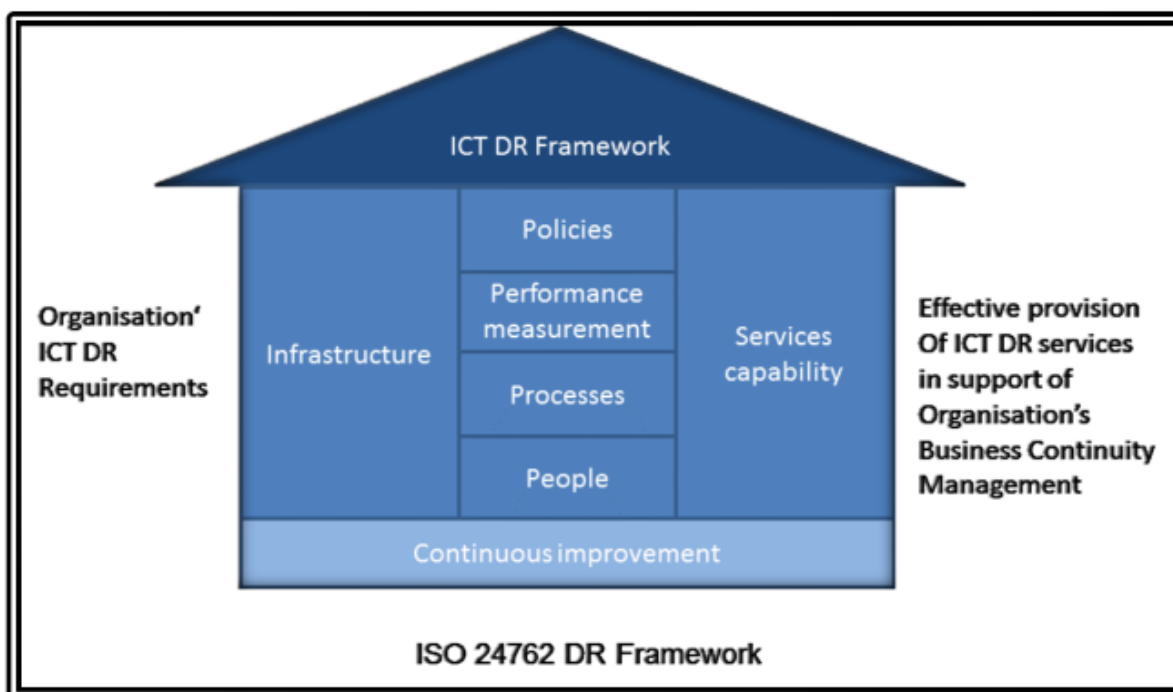


Figure 12: ISO 24762 DR framework

Information security management is the process by which management aims to achieve effective confidentiality, integrity and availability of information and service.

When an organisation implements ISMS the risks of interruptions to business activities for any reason should always be identified. ISO/IEC 27001 and ISO/IEC

27002 include a control objective for information security aspects of business continuity management (refer to Control Objective 14.1 in ISO/IEC 27002:2005), the implementation of which will reduce those risks. That control objective is supported by controls to be selected and implemented as part of the ISMS process. Business continuity management is an integral part of a holistic risk management process that safeguards the interests of an organisation's key stakeholders, reputation, brand and value creating activities through:



ICT GOVERNANCE FRAMEWORK

- identifying potential threats that may cause adverse impacts on an organization's business operations, and
- associated risks;
- providing a framework for building resilience for business operations;
- Providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures.

In planning for business continuity, the fall-back arrangements for information processing and communication facilities become beneficial during periods of minor outages and essential for ensuring information and service availability during a disaster or failure for the (complete) recovery of activities over a period of time. Such fall-back arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services.

A4.2.1. ISO/IEC 2472 CONTROLS

The standard lists specific requirements for ICT DR Service providers to continuously improve their ICT DR services.

ISO/IEC 24762 Controls		
Clause	Sec	Control Objective
	5.1	General
	5.2	Environmental stability
	5.3	Asset management
	5.4	Proximity of site
	5.5	Vendor management
	5.6	Outsourcing arrangements



ICT GOVERNANCE FRAMEWORK

ICT Disaster Recovery	5.7	Information security
	5.8	Activation and deactivation of disaster recovery plan
	5.9	Training and education
	5..10	Testing and ICT systems
	5.11	Business continuity for ICT DR services providers
	5.12	Business continuity for ICT DR services providers
ICT Disaster Recovery Facilities	6.1	General
	6.2	Location of recovery sites
	6.3	Physical access controls
	6.4	Physical security controls
	6.5	Dedicated areas
	6.6	Environmental controls
	6.7	Telecommunications
	6.8	Power supply
	6.9	Cable management
	6.10	Fire protection
	6.11	Emergency Operations Centre (EOC)
	6.12	Restricted facilities



ICT GOVERNANCE FRAMEWORK

	6.13	Non recovery amenities
	6.14	Physical facilities and support equipment life cycle
	6.15	Testing
Outsourced Service Provider's Capability	7.1	General
	7.2	Review organisation disaster recovery status
	7.3	Facilities requirements
	7.4	Expertise
	7.5	Logical access control
	7.6	ICT equipment and operation readiness
	7.7	Simultaneous recovery support
	7.8	Levels of service
	7.9	Types of service
	7.10	Proximity of service
	7.11	Subscription ratio for shared services
	7.12	Activation of subscribed services
	7.13	Organisation testing
	7.14	Changes in capability
	7.15	Emergency response plan
	7.16	Self-assessment



ICT GOVERNANCE FRAMEWORK

Selection of Recovery Sites	8.1	General
	8.2	Infrastructure
	8.3	Skilled manpower and support
	8.4	Critical mass of vendors and suppliers
	8.5	Local service providers' track records
	8.6	Proactive local support
Continuous Improvement	9.1	General
	9.2	ICT DR trends
	9.3	Performance measurements
	9.4	Scalability
	9.5	Risk mitigation

Table 7: Requirements for ICT DR Service providers

Signed By :

DATE:

Mr. EM Mzimela

MUNICIPAL MANAGER