ICT GOVERNANCE FRAMEWORK

Version 1.2 October 2021

© Copyright Reserved

Version Control and Approval			
Document Name	ICT GOVERNANCE FRAMEWORK		
Document Number/Version	Version 1.2		
Status/Revision History			
Rev #	**Revision Update**	**Revised By**	**Date**
1.0	New	Author: William Nkuna	May 2018
1.1	Revision	Author: Ray Mtetwa	December 2019
1.2	Revision	Author: Mpumelelo Khumalo	October 2021

Approval	
Date Approved	
Date Last Amended	October 2021
Date of Next Review	2021/22
Related Policies	ICT Security Policy
Authored By	
Name	Mpumelelo Khumalo
Position	Acting ICT Manager
Signature	Date: 30/03/2022
Reviewed and Recommended by	
Name	Ms. Sibongile Ngwenya
Position	Executive Manager: Corporate Services
Signature	Date: 30/03/2022
Name	Thamsanqa Mdontswa
Position	Chief Executive Officer
Signature	Date: 30/03/2022
Approved By	
Name	Ms. Portia Mushwana
Position	Chairperson: ICT Steering Committee
Signature	Date: 30/03/2022
Approved By	
Name	Chris Mudau
Position	Chairperson: Board and Accounting Authority
Signature	Date: 30/03/2022

© Copyright Reserved

Table of Contents

© Copyright Reserved

1 INTRODUCTION

1.1 ICT Governance Overview

The ICT Governance Institute (ITGI) defines ICT governance as "the leadership, organisational structures and processes that ensure that the enterprise's ICT sustains and extends the enterprise's strategies and objectives" (ITGI, 2003). In South Africa the Fourth King Report on Corporate Governance (King IV) highlights a category of corporate governance in the South African context, namely 'Technology and Information Governance' (IODSA, 2016). King IV, which became operational in South Africa on 1 November 2016, is a corporate governance report that is applicable to all South African entities, thus including public sector entities.

Principle 12 of the Governance principles of the King IV report (IODSA, 2016) stipulates the below:

The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives.

The table below lists the Technology and Information Governance recommended practices of the King IV report (IODSA, 2016).

Table 1: TECHNOLOGY AND INFORMATION GOVERNANCE PRINCIPLES

Practice 1	The governing body should assume responsibility for the governance of technology and information by setting the direction for how technology and information should be approached and addressed in the organisation.
Practice 2	The governing body should approve policy that articulates and gives effect to its set direction on the employment of technology and information.
Practice 3	The governing body should delegate to management the responsibility to implement and execute effective technology and information management.
Practice 4	The governing body should exercise ongoing oversight of technology and information management and, in particular, oversee that it results in the following: a. Integration of people, technologies, information and processes across the organisation. b. Integration of technology and information risks into organisation-wide risk management. c. Arrangements to provide for business resilience. d. Proactive monitoring of intelligence to identify and respond to incidents, including cyber-attacks and adverse social media events. e. Management of the performance of, and the risks pertaining to, third-party and outsourced service providers. f. The assessment of value delivered to the organisation through significant investments in technology and information, including the evaluation of projects throughout their life cycles and of significant operational expenditure.

© Copyright Reserved

	g. The responsible disposal of obsolete technology and information in a way that has regard to environmental impact and information security. h. Ethical and responsible use of technology and information. i. Compliance with relevant laws.
Practice 5	The governing body should exercise ongoing oversight of the management of information and, in particular, oversee that it results in the following: a. The leveraging of information to sustain and enhance the organisation's intellectual capital. b. An information architecture that supports confidentiality, integrity and availability of information. c. The protection of privacy of personal information. d. The continual monitoring of security of information.
Practice 6	The governing body should exercise ongoing oversight of the management of technology and, in particular, oversee that it results in the following: a. A technology architecture that enables the achievement of strategic and operational objectives. b. The management of the risks pertaining to the sourcing of technology. c. Monitoring and appropriate responses to developments in technology, including the capturing of potential opportunities and the management of disruptive effects on the organisation and its business model.
Practice 7	The governing body should consider the need to receive periodic independent assurance on the effectiveness of the organisation's technology and information arrangements, including outsourced services.
Practice 8	The following should be disclosed in relation to technology and information: a. An overview of the arrangements for governing and managing technology and information. b. Key areas of focus during the reporting period, including objectives, significant changes in policy, significant acquisitions and remedial actions taken as a result of major incidents. c. Actions taken to monitor the effectiveness of technology and information management and how the outcomes were addressed. d. Planned areas of future focus.

Technology and Information Governance exists to inform and align decision making for ICT planning, policy and operations in order to meet business objectives, ascertain that risks are managed appropriately and verify that resources are being used responsibly and strategically. Because ICT services account for significant capital and operational expenses in most organizations, the formal processes within a governance framework ensure that business requirements ultimately drive planning decisions for the development and management of ICT resources. Formalizing governance processes also helps ensure that technology

© Copyright Reserved

business leaders are in agreement on what is an appropriate level of risk in the ICT that powers day-to-day operations.

This document represents and outlines an ICT governance framework for the SASSETA that meets the unique needs of government customers and at the same time provides the structure to successfully manage a complex ICT environment and results in services that add value to, and make successful the business of government.

2 LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards. The following legislation, among others, were considered in the drafting of this policy:

a) Constitution of the Republic of South Africa Act, Act No. 108 of 1996.

b) Copyright Act, Act No. 98 of 1978.

c) Electronic Communications and Transactions Act, Act No. 25 of 2002.

d) Minimum Information Security Standards, as approved by Cabinet in 1996.

e) Public Finance Management Act.

h) National Archives and Record Service of South Africa Act, Act No. 43 of 1996.

i) Promotion of Access to Information Act, Act No. 2 of 2000.

j) Protection of Personal Information Act, Act No. 4 of 2013.

k) Regulation of Interception of Communications Act, Act No. 70 of 2002.

l) Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005. The following internationally recognised ICT standards were leveraged in the development of this policy:

m) Control Objectives for Information Technology (COBIT) 5, 2012.

n) ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls.

o) King IV Code of Governance Principles, 2016.

2.1 King IV report and the public sector

One of the fundamental principles of the King IV report is the message of social responsibility that companies have for the people of the country – especially the community in which they operate (IODSA, 2016). This corresponds with the vision of the South African National Government to improve service delivery to all, as well as with the Batho Pele principles (PWC, 2009; PWC, 2010b), which were introduced in 1997 and set the scene for corporate governance principles on local authority level (DPSA, 1997). The most important aspect of a public sector entity is the delivery of a specific service to the citizens in order to improve the

© Copyright Reserved

quality of life for all (Woods, 2010). The particular service(s) need to be delivered in a sustainable way and public sector entities in South Africa are under pressure to advance in service provision. This is however only possible if public sector entities are able to utilise their ICT assets in a modern and effective way, to reap the required benefits. The South African government acknowledges that ICT is integral in reaching the community and delivering services in a more effective manner (PWC, 2010b) – thus ICT functions as the enabling agent. By being more efficient, money could be saved and invested directly to the benefit of citizens. The South African national government incorporated the E- government programme as part of their Vision 2014 priorities (PWC, 2010b) – not in a traditional way as hardware and software, but as a vehicle to improve service delivery and creating access for all (ITGI, 2003; Le Roux,2010:50; PWC, 2010b). Local authorities are obliged to improve service delivery, be cost-effective and keep up to date with innovative technology trends. After ICT was identified as a fundamental element of running a business and hence the introduction of ICT governance in the King IV report, it was emphasised that local authorities should prioritize ICT as an important strategic asset and include it when determining the road forward as well as in identifying risks (PWC, 2009). By implementing the ICT governance principles contained in the King IV report these issues can be addressed (Woods, 2010).

2.2 Process and objective of the framework

The Framework is, by its nature, a living document that will be adjusted as processes change and mature. The requirement of principle 12 of the King IV report stipulates that an alignment exercise between ICT and the business operations of the entity should be performed in order to reach the objectives of the entity. Therefore, not only is insight needed into the organizational environment and processes, but also into the ICT environment, consisting of ICT architecture and ICT processes.

By adopting the ICT governance framework, the following objectives are anticipated:

a) Raising the profile of ICT within SASSETA
b) Raising the profile of ICT as a strategic enabler for effective administration and service delivery
c) Bringing international good practices into the SASSETA
d) Further strengthening corporate governance of ICT as well as ensuring that ICT be an integral part of the strategic direction of the SASSETA
e) Institutionalizing ICT governance as an integral part of SASSETA corporate governance.
f) Creating a process whereby ICT governance standards across and within the local government sector can be introduced
g) Improving the ICT governance literacy and lingo within SASSETA.

2.3 Organisational imperatives

Based on the nature of the entity, any entity has specific business imperatives (Boshoff, 2010). Boshoff defines a business imperative as a non-negotiable prerequisite principle, imposed by management, which needs to be achieved in order to enable the company to reach its strategic business objectives in the specific environment. Six imperatives were identified as the key business imperatives for a public sector entity Table 2 identifies the

© Copyright Reserved

business imperatives for a public sector entity and provides a brief description of the imperative from a business requirements perspective.

Table: 2: Business imperatives for a public sector entity

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

When aligning the ICT environment with the business objectives of the entity as required by principle 12 of the King IV report, the ICT environment should therefore be aligned with these business imperatives (IODSA, 2016).

2.4 Aligning organisational imperatives with the ICT environment

The impact of the business imperatives of the public sector (identified in Table 2) on the ICT environment, were evaluated and recorded in Table 3 below. This table provides the last step towards achieving the alignment between the ICT environment and the business objectives of the entity as required by principle 12 of the King IV report. A golden line was created from the nature of the entity to the impact thereof on the clusters of the ICT environment, resulting in alignment between the business processes and goals and the ICT environment.

© Copyright Reserved

Table: 3: Operational imperatives: ICT environment perspective

Imperative	Operational Requirements	ICT Environment	Clusters Impacted
Affordability	Public sector entities require ICT costs to be low and are focused on value for money. The benefits received from the ICT environment should outweigh the costs. Costs of ownership and operating costs should be low in order to utilize taxpayers' money efficiently in transforming it into tangible outcomes for society.	The cost of ownership of particular ICT software and hardware needs to be as low as possible. This includes the initial purchase price, annual license fees and the costs associated with upgrades and maintenance.	Applications Hardware Networks
Agility	The ICT systems should be able to adapt to changes in political power, restructuring possibilities and changes in the economy. ICT should also be able to adapt to easier methods of interactions with the public.	The hardware and applications need to facilitate various systems, since a public sector entity is diverse in its trade and has various stakeholders. ICT should be easy to upgrade and maintain the system.	Applications Hardware
Ease of use	The ICT technology should be easy to use for all users. A complex system is not desirable as it could lead to idle time, mistakes and the appointment of highly skilled staff. Decisions are made based on information captured and therefore it is important to limit errors. The entities also want to limit the expenditure of ICT training required by complex systems.	The user interface should generate an experience for users that is not demoralizing. The response rate and the content should encourage users to finalise tasks quickly and effectively. The business process should be logical, prompting for the next procedural step, require the successful completion of a step before the user can move to the	Applications
Reliability	Systems need to functions as intended at all times, thereby being available, effective and efficient.	The systems should be of a reliable quality to avoid malfunctioning. The systems should also be able to adjust to unexpected changes with minimal damage. A detailed contingency plan should be in place. A continual monitoring system that monitors availability of systems	Applications Hardware Networks
Security	Unauthorized access to the personal data of citizens should be prevented.	Data must be kept in a valid, accurate and complete manner. Appropriate firewalls, anti-virus programs and facilitation of administrators' rights should be in	Applications Hardware Networks
Self-Service	Entities want citizens to be able to perform certain tasks directly and quickly themselves.	Online functionality should be developed and activated. User-friendly interfaces should be used to eliminate errors. A help function should be available and users should be guided step-by-step in a logical manner.	Applications

3 Performance Measurement

Performance measures are required to ensure that the outcomes of ICT activities are aligned to the organisation's goals. Internal ICT process measures are required to ensure that the processes are capable of delivering the intended outcomes cost-effectively. Advanced performance measurement enables the measurement of key aspects of ICT capability such as creativity and agility (new ideas, speed of delivery and success of a change programme), development of new solutions, ability to operate reliable and secure services in an increasingly demanding ICT technical environment, and the development of human resources and skills.

© Copyright Reserved

3.1 Current ICT Key Performance Indicators (KPIs)

The ICT Strategic Outcomes and Programmes are included in the SASSETA ICT Strategy (Master Systems Plan) - CGICT_ICT_MSP. The Strategic outcomes and programmes include key indicators for ICT performance in supporting the overall Business Strategy and Government Programmes.

3.2 Management of the Governance Process

The goal of governance is to facilitate agile, effective and transparent decision making. This requires consistent and timely communications. Stakeholders that may be impacted by decisions must have a way to know what decisions are in a queue at any given point in time and understand how to provide feedback. To facilitate this process, an ICT Steering Committee comprising of executive, organisational and ICT Management needs to be in place. The role of the committee is to:

- Determine prioritization of ICT-enabled investment programs in-line with the SASSETA business strategy and priorities
- Track status of projects and resolve resource conflict
- Monitor service levels and service improvements The Executive / Senior management must:
- Ensure that ICT goals are aligned with the SASSETA strategic goals and support processes.
- ICT strategy is integrated with strategic business processes and that related risks are managed.
- Significant ICT investment and expenditure are informed by the SASSETA enterprise architecture, motivated, monitored and evaluated.
- Advice is provided to the Accounting Officer on the implementation and management of the Corporate Governance of ICT.

3.3 Communications

Communications of governance processes and outcomes will be shared not only with the ICT community but with the organizational leadership affected by the management of ICT. Regular governance communications regarding key governance activities, policies and decisions will be reported to the key leadership group that regularly meet for information sharing. For more targeted customer communications, the Network Administrator will play a primary role in keeping management informed of ICT Governance decisions that will affect ICT services and projects, and will serve as the primary contact for organization-based ICT planning and the resulting comprehensive service agreements.

4 ICT Governance Framework: Primary Roles

4.1 Role of the CEO/ICT Manager

The CEO, is accountable:

a) For all transactions entered into by his/her designates.

b) For sound record management (Information Management)

The CEO may delegate certain duties to the Chief Financial Officer/Executive Manager (Corporate Services), who would be accountable to him/her.

© Copyright Reserved

Following the intentions of King IV, it is suggested that;

a) The CEO's ICT function, reside under the Corporate Services function.

b) The implementation of the governance of ICT is delegated from the Corporate Services function to the ICT Steering Committee made of the relevant executive / senior management, as well as the SASSETA ICT Management.

The ICT Manager is responsible for the implementation and operation of ICT governance and is expected to report to the ICT Steering Committee and the council about the effective and efficient management of ICT resources to facilitate the achievement of corporate objectives.

King IV also requires the CEO/ICT Manager to define maintain and validate the ICT value proposition. Align ICT activities with environmental sustainability objectives, implement an ICT control framework and ensure all parties in the chain from supply to disposal of ICT goods and services apply good governance principles.

4.2 Role of the ICT Steering Committee

The SASSETA ICT Steering Committee is to ensure that everyone in the SASSETA understands the link between the organisation and the ICT goals and accepts their responsibilities with respect to the supply and demand for ICT. The SASSETA ICT Steering Committee will ensure that:

a) Develop corporate level ICT strategies and plans that ensure the cost-effective application and management of ICT systems and resources throughout the SASSETA;

b) Monitor and review current and future technologies to identify opportunities to increase the efficiency of ICT resources;

c) Monitor and evaluate ICT projects and achievements against the ICT Strategic Plan;

d) Develop and review standards, policies and procedures; and

4.3 Role of the customer

The customers of ICT services (the departmental heads of SASSETA) have a critical role in the governance process for ICT. Primarily, the customer is concerned with what ICT delivers, how ICT will meet program needs, and how well ICT performs.

The customer's most prominent role therefore is Customer Strategic Planning, the on-going internal planning between departmental heads and ICT Management, to determine the technological needs for given projects, priorities, programs and annual budgets. Based on an ongoing relationship between SASSETA departmental heads and ICT Management, they determine the ICT needs of the SASSETA based on business strategic planning. The ICT Manager serves as the responsible party for ensuring that the resulting ICT services – regardless of sourcing – are meeting the needs of the organization.

5 Risk Management

The management of risks is a component of ICT Governance ensuring that the strategic objectives of the business are not jeopardised by ICT failures. ICT related risks are increasingly

© Copyright Reserved

an ICT Steering Committee level issue as the impact on the organisation of an ICT failure, be it an operational crash, security breach or a failed project, can have devastating consequences. However, managing ICT risks and exercising proper governance is a challenging experience for business managers faced with technical complexity, a dependence on an increasing number of service providers, and limited reliable risk monitoring information. As a consequence, management is often concerned whether risks are being cost effectively addressed, and they need assurance that risks are under control.

Therefore, the steering committee should manage enterprise risk by:

a) Ascertaining that there is transparency about the significant risks to the enterprise and clarifying the risk- taking or risk- avoidance policies of the enterprise.

b) Being aware that the final responsibility for risk management rests with the steering committee so, when delegating to executive management, making sure the constraints of that delegation are communicated and clearly understood.

c) Being conscious that the system of internal control put in place to manage risks often has the capacity to generate cost- efficiency.

d) Considering that a transparent and proactive risk management approach can create competitive advantage that can be exploited.

e) Insisting that risk management is embedded in the operation of the enterprise, responds quickly to changing risks and reports immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).

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

5.1 What are the risks?

To enable effective Governance, ICT risks should always be expressed in the business context rather than in the technical language favoured by ICT risk experts. Business risks are affected by the business environment (management style, culture, and risk appetite, industry sector factors such as competition, reputation etc., national and international regulations). ICT risks can be similarly affected. There is no single accepted set of generic ICT risk definitions, but these headings can be used as a guide (Taken from a global study by the Economist Intelligence Unit in 2002):

a) Investment or expense risk
b) Access or security risk
c) Integrity risk
d) Relevance risk
e) Availability risk
f) Infrastructure risk
g) Project ownership risk

© Copyright Reserved

For ICT to be effectively governed, top management must be able to recognise ICT risks and ensure that significant risks are managed. Significance of an ICT risk is based on the combination of impact (what effect the risk would have on the organization if it occurred) and likelihood (the probability of the risk occurring). Because of the complexity and fast changing nature of ICT, education and awareness is essential to ensure risks are recognised – not just at the top management level but at all levels throughout the organisation. It is increasingly common for a dedicated risk management function to be established or for external advice to be obtained on a regular basis to ensure that risks are monitored and the rest of the organisation is kept informed.

Maintenance of a risk catalogue or risk register can be helpful to ensure that a thorough review of all ICT related risks takes place on a periodic basis and for providing assurance to management that risks are being addressed. Currently our Internal Audit and Risk Management section manage and monitor all risks within the organization, including ICT ones.

5.2 When to outsource

Acquiring ICT Governance competence from outside the organisation will be driven by two different objectives:

a) When it is more cost-effective to outsource skills that are not available in-house

b) When outside input of expertise is beneficial in its own right

However, if implementation of ICT Governance is to be successful and sustainable, competence will have to be developed within the organisation, since management of ICT must be owned within the organisation. In many organisations where all or significant parts of the ICT service have been outsourced, responsibility and competence for controlling use of these services should still be retained internally. It is essential to retain sufficient skills internally to be able to sustain the business and to understand and manage what is being outsourced.

6 ICT and Audit

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

6.1 What are the roles of ICT and Audit for ICT Governance?

Role of ICT Audit

a) ICT Governance is a management responsibility, and therefore not the sole responsibilities of an Audit function

© Copyright Reserved

b) ICT Governance requires management commitment and ownership within ICT and the business in order to make it happen. Audit can then determine if it is happening, and provide assurance to the board.
c) When reviewing Governance, Audit must do more than just identify problems. They need to identify root causes and make constructive recommendations.
d) Audit can test controls especially where control is critical and assurance is required. But increasingly there is a trend for ICT to "test themselves" by performing self- assessments.
e) Audit can play a part in setting standards, and providing control criteria and control benchmarks, particularly in respect of external regulation.

Role of ICT

a) ICT has to be responsible for changing the culture of the ICT organisation, for managing the ICT processes, and adopting a focus on controls.
b) Education in control principles may be needed, and audit can help with this by working together with ICT and by providing training, workshops and staff secondments.
c) A common framework and understanding is needed in order to ensure that ICT Management is exercising ICT Governance.
d) ICT should take a lead on governance; audit can "sow the seeds".
e) If ICT (as so often) is in `fire fighting` mode it is harder for them to drive governance.

7 Information Security

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

The view of the impact ICT Governance is that Information security concerns have increased due to:
a) Technical complexity
b) Hackers and virus spreaders
c) Increasing ease of use, and the accessibility of ICT systems
d) Anywhere/anytime access

Proper governance of security, like any other aspect of ICT, requires top management to be more involved in setting direction and overseeing the management of risk. It is essential therefore to take action to ensure that:

a) The importance of information security is communicated to all and that [illegible] underpin activities in a changing environment.

© Copyright Reserved

b) The ownership and responsibility for information security is accepted by senior management in the business as well as in ICT.

c) The security function is there to assist management and security is ultimately the responsibility of everyone.

d) Any shortage of skilled resource in this area is addressed, as it may be impossible to retain all the necessary skills and functions in- house.

e) Responsibility for any security aspects of corporate compliance is accepted by the Steering Committee.

7.1 Roles and Responsibilities

For information security to be properly addressed, greater involvement of the organisation is required.

For information security to be properly implemented, skilled resources such as information systems auditors, security professionals and technology providers need to be utilized.

An Information Security Officer (ISO) should be in place as an advisor to management and the project owner of security action plan. The role can be part time and is often supported by external advisors. It is often part of a Risk Management function. An Operational Team will be needed to maintain and monitor security processes and operate administrative procedures. The Audit Function plays a key independent role in monitoring and assessing the adequacy of security within the organization.

8 Communication Management

SASSETA must have documented standards, procedures or guidelines for the management/administration of their network. Critical system environments must be restricted from the general user environments by implementing virtual private network. Firewalls must be used to inspect traffic passing through the network and the firewall logs are actively monitored and managed in-house.

Intrusion detection system (IDS) and intrusion prevention system (IPS) must be in use. Security systems must be actively monitored and their logs must be not be edited. The SASSETA must use anti-virus software to detect and prevent electronic viruses.

The SASSETA must have patch management framework in place to prevent against systems vulnerabilities being compromised. If the SASSETA allows wireless access it must be appropriately controlled or/and managed.

Dealing with an information breach is not only embarrassing but also has legal implications since there are notification requirements if sensitive employee, service provider, or learner data is accessed inappropriately or potentially exposed to a breach. The development of a patch management strategy is therefore critical for the SASSETA to:

a) determine the methods of obtaining patches
b) specify methods of validating patches

© Copyright Reserved

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

9 Wireless

Wireless is a great technology that offers many benefits and requires great responsibility. A responsibility that is unfortunately much too often ignored when implementing it. A wireless network needs to be properly secured as it poses a number of extremely serious risks and dangers if left wide open and exposed, which many users are unaware of such as:

a) Bandwidth Parasite: Where the intruders uses the victims Broadband connection to get online without paying. This will not cause any direct harm to the compromised network, but it can slow down internet or network access for the victim.

b) Masking Criminal Activity: Where an unauthorized user could abuse the victim's connection for malicious purpose like hacking, launching a DOS attack, or distributing illegal material.

c) Free Access to Private Data: A wireless network is also a direct backdoor into the victim's private network literally. Instead of intruding from the public side of the gateway device, the intruder connects directly to the network on the private side of the gateway device, completely bypassing any hardware firewall between the private network and the broadband modem. The intruder can completely take advantage of this by snooping around undisturbed and getting access to confidential data. It is therefore imperative that SASSETA should develop policies and procedures that will govern the security of their wireless.

10 Problem Management

The SASSETA must have operational procedures for the management of faults/incidents in the use or implementation of ICT services that users, third parties and contractors were aware of. It m u s t also indicate that the documented procedures must address planning and preparation, detection, initiation, evaluation containment, eradication, response, recovery, closure post incident.

Incidents must be tracked to identify trends and underlying causes of operational failures with the view to long term solutions.

The SASSETA needs to have emergency response process for dealing with serious incidents.

The process includes:

a) definition of an emergency situation or incident
b) detailed description of roles and responsibilities
c) defined response process allowing critical decision to be made quickly
d) defined steps to be taken in emergency situations

© Copyright Reserved

e) contact details for all key personnel

The SASSETA should enforce good practices in the management of problems/incidents. Management should ensure that they harmonise the discord that currently exist between procedures and processes.

11 Asset Management

The SASSETA must have internal controls over the management of information assets appeared satisfactory. The SASSETA must keep an asset register, which requisite to be updated regularly and when changes occur. The asset register held important information about each asset such as asset owner, asset location, and date of acquisition. The SASSETA should protect the asset register from unauthorized changes by limiting access rights.

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

12 Business Continuity Management

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

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

13 ICT Governance Framework Decision Making Process

While the ICT Manager (through delegation by the CEO) remains solely accountable to both customers and stakeholders for all ICT direction, policy and strategy on an executive level, the ICT Governance Framework reflects the changes in roles and responsibilities brought on by consolidation and adopts strategies to ensure customer business leadership participation and buy- In.

a) The ICT Steering Committee will serve as the most diverse governance body both in representation (including organizational leadership and employee representation) and in scope of advice and consultation.

© Copyright Reserved

b) The ICT Manager will maintain a flexible governance process, particularly in the areas of vision and planning and the formation of additional formal or informal groups in a fashion that improves the decision-making process and the outcomes for the SASSETA's ICT.

13.1 Decision Rights

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

SASSETA's ICT Governance Framework utilizes the Responsibility Assignment Matrix to define decision rights. Roles in this decision-making framework, commonly referred to as RACI Matrix, fall into one of four distinct categories:

- Responsible (R),
- Accountable (A),
- Consulted (C),
- Informed (I).

a) Responsible: Those that do the work to fulfill the deliverables. A Responsible person or persons get their authority from the individual that is accountable. In SASSETA's ICT Governance Framework, the CEO delegates responsibility to the teams in this framework.

b) Accountable: The one person that has ultimate decision-making authority and is answerable for the correct and thorough completion of deliverables. This person can delegate responsibility for completion of the deliverables to others, but remains accountable. In SASSETA's ICT Governance Framework, the CEO is solely accountable to both customers and stakeholders for all ICT decisions and activities in the in the SASSETA environment.

c) Consulted: Those whose opinions are sought, typically subject matter experts and advisors. There is two-way communication between individuals that are consulted and those responsible.

d) Informed: Those that are kept up to date on progress, often only on completion of the deliverables.

13.2 Roles and Responsibility Categories

- Strategic: CEO, and Corporate Services Executive
- Tactical: ICT Manager, ICT Officers
- Operational Business Process Owner

13.3 Vision, Planning and Operations Governance

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

© Copyright Reserved

Principles	Recommended Practice
The Steering Committee should be responsible for ICT (ICT) governance.	• The Steering Committee should assume the responsibility for the governance of ICT and place it on the Steering Committee agenda • The Steering Committee should ensure that an ICT Charter and Policies are established and implemented • The Steering Committee should ensure promotion of an ethical governance culture and awareness and of a common ICT Language. • The Steering Committee should ensure that an ICT internal control framework is adopted and implemented • The Steering Committee should receive independent assurance of the effectiveness of the ICT internal controls
ICT should be aligned with the performance and sustainability objectives of the company	• The Steering Committee should ensure that the ICT Strategy is integrated with the company's strategic and business processes • The Steering Committee 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 ICT.
The Accounting Officer should delegate to management the responsibility for the implementation of an ICT Governance Framework	• Management should be responsible for the implementation of the structures, processes and mechanisms for the ICT Governance framework • The Accounting Officer may appoint an ICT Steering Committee of similar function to assist with its governance of ICT. • The Accounting Officer should appoint Director/Network Administrator responsible for the management of ICT • The Director/Network Administrator should be a suitably qualified and experienced person who should have access and interact regularly on strategic ICT matters.
The Steering Committee should monitor and evaluate significant investments and	• The Steering Committee should oversee the value delivery of ICT and monitor the return on investment from significant ICT projects.

© Copyright Reserved

expenditure	• The Steering Committee should ensure that intellectual property contained in information systems is protected. • The Steering Committee should obtain independent assurance on the ICT governance and controls supporting outsourced ICT services.
ICT Should form an integral part of the organisation's risk management	• Management should regularly demonstrate to the Steering Committee that the company has adequate business resilience arrangements in place for disaster recovery • The Steering Committee should ensure that the organisation complies with ICT laws and that ICT related rules, codes and standards are considered.
The Steering Committee should ensure that information assets are managed effectively	• The Steering Committee should ensure that there are systems in place for the management of information which should include information security, information management and information privacy. • The Steering Committee should ensure that all personal information is treated by the company as an important business asset and is identified. • The Steering Committee should ensure that an Information Security Management System (based on the ISO/IEC 27002 standards of **plan, do, check** and **act** approach) is developed and implemented • The Steering Committee should approve the information security strategy and delegate and empower management to implement the strategy.
A Risk committee and audit committee should assist the Steering Committee in carrying out its ICT responsibilities	• The risk committee should ensure that ICT Risks are adequately addressed. • The risk committee should obtain appropriate assurance that controls are in place and effective in addressing ICT risks • The audit committee should consider ICT as it relates to financial reporting and the going concern of the company. • The Audit committee should consider the use of technology to improve audit coverage and efficiency.

13.4 Defined Processes

The ICT Steering Committee was established to provide advice to the CEO/ICT Manager. The ICT Steering Committee serves the CEO/Executive Manager – Corporate Services who can then delegate to the ICT Manager in a consultative capacity. The committee is required to advise the CEO/ICT Manager on a broad array of topics including, but not limited to:

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

© Copyright Reserved

The ICT Steering committee meetings and agenda are managed by the office of the ICT Manager.

To fulfill its diverse statutory responsibilities, the ICT Steering committee will conduct ongoing meetings to gain an understanding of and provide insight into key technology decisions.

Agendas for ICT steering committee meetings will include regular reports on governing activity and decision points as well as significant management decisions that do not flow through governance, such as budgeting and rate setting of ICT Services.

13.5 The ICT Steering Committee

The purpose of the ICT Steering Committee is, as a group responsible for providing executive leadership in the development of standards, policies, and the prioritization of various initiatives.

The Executive IT Steering Committee will provide a stabilizing influence so organizational concepts and directions are established and maintained with a visionary view. The Steering Committee provides direction on long-term strategies in support of the SASSETA's mandates and business vision. Members of the Steering Committee ensure that the SASSETA's Information Technology needs and objectives are being adequately addressed.

13.6 ICT Steering Committee Responsibilities

The IT Steering Committee is responsible for:

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

Refer to the ICT Steering Committee Terms of Reference for detailed responsibilities.

13.7 ICT Steering Committee Membership

It is critically important to have key stakeholders involved in the Steering Committee. These stakeholders are representatives from both the business as well as IT. It is recommended the ICT Steering Committee comprise of the following persons or representative thereof:

a) CEO/CFO
b) Chairperson of the ICT Steering Committee
c) Executive Manager – Corporate Services ;
d) Departmental Managers
e) ICT Manager
f) Any other employee deemed necessary for the function of the ICT steering committee

13.8 Frequency and Scheduling Meetings

The Chairperson will schedule meetings to take place as and when necessary, but the committee must meet quarterly or at least four times a year.

© Copyright Reserved

14 Reference List

a) Boshoff, W. 2010. IT Governance and IT Assurance. Masters in Commerce (Computer Auditing) lecture slides, University.

b) DPSA (Department for Public Service and Administration). 1997. Batho Pele – Together beating the drum for service delivery [Online]. Available: http://www.dpsa.gov.za/batho-pele/Principles.asp [2011. July 21].

c) IODSA (Institute of Directors Southern Africa). 2016. King Report on corporate governance for South Africa (King IV) [Online]. Available: http://www.iodsa.co.za [2020, Feb 05].

d) ISACA (Information Systems Audit and Control Association). 2008. Top business/technology issues - Survey results [Online]. Available:

http://www.isaca.org/Knowledge-Center/Research/Documents/Top- Business-

Technology-Survey-Results.pdf [2011, July 20].

e) ITGI (IT Governance Institute). 2003. Board briefing on IT governance [Online]. Available: http://www.itgi.org [2011, May 24].

f) ITGI (IT Governance Institute). 2005. IT alignment: Who is in charge? [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/ITAlignment- Who-Is-in-Charge.pdf [2011, June 8].

g) ITGI (IT Governance Institute). 2008a. Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit

h) – A management briefing from ITGI and OGC [Online]. Available: http://www.itgi.org/template_ITGI275e.html?Section=Recent_Publications&Template

i) =/TaggedPage/TaggedPageDisplay.cfm&TPLID=43&ContentID=14046 [2011, May 25].

j) ITGI (IT Governance Institute). 2008b. IT governance global status report – 2008 [Online]. Available: http://www.isaca.org/Knowledge- Center/Research/Documents/ITGI- Global-Status-Report-2008.pdf [2011, June 8]. Langeberg University http://scholar.sun.ac.za

k) ITGI (IT Governance Institute). 2008c. Understanding how business goals drive IT goals [Online]. Available: http://www.isaca.org/Knowledge- Center/Research/Documents/Understand-Bus-Drive-IT- Goals-15Oct08- Research.pdf [2011, June 8].

l) IT governance Institute (ITGI). 2011. Global status report on the governance of IT (CGEIT) – 2011 [Online]. Available: http://www.isaca.org/Knowledge- Center/Research/Documents/Global-Status- Report-GEIT-10Jan2011 -Research.pdf [2011, July 23].

m) ITGI & OGC (IT Governance Institute & Office of Government Commerce). 2005. Aligning Cobit, ITIL and ISO 17799 for business benefit: Management summary [Online]. Available: http://www.itgovernance.co.uk/files/ITIL-COBiTISO17799JointFramework. pdf [2011, May 26 25]. PWC (PricewaterhouseCoopers). 2009. King's Counsel. King IV: A municipal perspective – at a glance [Online]. Available: http://www.pwc.com/za/en/publications/steering-point.jhtml#SteeringPoint [2011, May 26].

© Copyright Reserved

n) Le Roux, F. 2010. The applicability of the Third King Report on Corporate Governance to small and medium enterprises [Online]. Available: http://www.scholar.sun.ac.za/handle/10019.1/1017 [2011, May 25].

o) PWC (PricewaterhouseCoopers). 2010a. IT governance [Online]. Available: http://www.pwc.com/za/en/publications/steering-point.jhtml [2011, May 26]. Langeberg University http://scholar.sun.ac.za

p) PWC (PricewaterhouseCoopers). 2010b. King's Counsel. Understanding and unlocking the benefits of sound corporate governance in government and the public sector [Online]. Available: http://www.pwc.com/za/en/publications/steeringpoint. jhtml#SteeringPoint [2011, May 26].

q) PWC (PricewaterhouseCoopers). 2010c. King IV and related legislative requirements [Online]. Available: http://www.pwc.com/za/en/publications/steeringpoint [2011, May 26].

r) Woods, S. 2010. Governing IT in the public sector [Online]. Available: http://www.itnewsafrica.com/2010/08/governing-it-in-the- public-sector/ [2011, May 26].

© Copyright Reserved