



the dpsa

Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

PUBLIC SERVICE CORPORATE
GOVERNANCE OF INFORMATION
AND COMMUNICATION
TECHNOLOGY

POLICY FRAMEWORK

Version 2

March 2022

TABLE OF CONTENTS

PREFACE	i
EXECUTIVE SUMMARY.....	i
GLOSSARY OF TERMS AND DEFINITIONS.....	ii
1. PURPOSE.....	1
2. SCOPE.....	1
3. REGULATORY FRAMEWORK.....	2
4. APPLICABILITY	2
5. BACKGROUND	2
6. INTRODUCTION.....	3
7. OBJECTIVES OF POLICY FRAMEWORK	3
8. BENEFITS OF CORPORATE GOVERNANCE OF ICT	4
9. CORPORATE GOVERNANCE OF ICT IN THE PUBLIC SERVICE	4
9.1 Corporate governance.....	4
9.2 Corporate governance of ICT.....	5
10. LAYERED APPROACH TO CORPORATE GOVERNANCE OF ICT.....	5
11. ACCOUNTABILITY STRUCTURE FOR CORPORATE GOVERNANCE OF ICT	6
11.1 Governance structures.....	6
11.1.1 EXCO.....	6
11.1.2 ICT steering committee.....	7
11.2 Roles and Responsibilities.....	8
11.2.1 Head of Department	8
11.2.2 Head of ICT	8
12. POLICY FRAMEWORK FOR CORPORATE GOVERNANCE OF ICT IN THE PUBLIC SERVICE	9
13. PRINCIPLES AND PRACTICES.....	10
14. CORPORATE GOVERNANCE OF ICT SYSTEM.....	14
15. IMPLEMENTATION OF A CORPORATE GOVERNANCE OF THE ICT SYSTEM	15
15.1 Business enabling policies, frameworks, and plans.....	16
16. ICT ALIGNMENT PLANNING	18
17. MONITORING AND EVALUATION.....	19
18. GOVERNMENT-WIDE ICT PROJECT GOVERNANCE MECHANISM	19

19. NON-COMPLIANCE	20
20. CONCLUSION	20
21. REFERENCES.....	21

PREFACE

The functions of the Minister of Public Service and Administration as enshrined in the Public Service Act, 1994 include the responsibility to develop the norms and standards for governance and management of electronic government in the public service. The Public Service Regulations, 2016 support the Act by directing the executive authority and head of a department to prepare a strategic plan and information and communication technology plan, respectively.

These arrangements intend to strengthen information and communication technology (ICT) utilisation to support the achievement of the departmental targets and objectives by fostering the involvement of executive management in all important ICT decisions. This accountability enables the department to align the delivery of ICT services with the department's strategic goals.

The Public Service Corporate Governance of ICT Policy Framework version 2 ("Policy Framework") seeks to provide the departments with direction to implement corporate governance of ICT within their sphere of accountability and responsibility. The leadership should provide the necessary business enabling policies, frameworks plans, structures, and other relevant resources.

EXECUTIVE SUMMARY

The Policy Framework supports the Medium Term Strategic Framework 2019 – 2024, Priority 1: Building a capable, ethical and developmental state through e-government to improve service delivery.

Effective Corporate Governance of ICT is essential to ensure that ICT supports business goals, ensures benefit realization from ICT expenditure, and appropriately manages ICT-related business risks and resources.

The existing Policy Framework that the Cabinet approved in 2012 focuses mainly on compliance with no performance considerations. This weakness was confirmed by the repeat audit findings of the Auditor-General of South Africa (AGSA) on IT governance weaknesses where IT projects do not meet the business expectations.

The revised Policy Framework has been primarily developed to address performance shortcomings. It directs the strategic leadership of the department (executive management) to take responsibility for the governance of ICT equivalent to the other departments, including but not limited to finances and human resources.

This Policy Framework aligns with the new developments that occur after the approval of the current Policy Framework, including but not limited to:

- Public Service Regulations, 2016;
- King IV code; and
- COBIT 2019.

The implementation of this Policy Framework will be supported by implementation guidelines and templates issued by the Department of Public Service and Administration (DPSA).

GLOSSARY OF TERMS AND DEFINITIONS

TERM	DEFINITION
AGSA	Auditor-General of South Africa
Applicability	Appositeness, appropriateness, relevance, pertinence, relatable, affiliation
Assessment Standard	Corporate Governance of ICT Assessment Standard
Business	The business of the department refers to the department's core activities and internal support activities
CGICTPF	Corporate Governance of ICT Policy Framework This term in this revised Policy Framework will also mean governance of ICT, IT governance, and Enterprise governance of Information & Technology. This approach recognizes that other global best-practice frameworks use these terms interchangeably.
Corporate	Public service-wide level: a group of related departments enabling the public service to achieve its strategic mandate. Departmental level: a group of related components enabling the department to achieve its strategic mandate. For this Policy Framework, corporate means the same as an enterprise.
Corporate governance	King IV defines corporate governance as the exercise of ethical and effective leadership by the governing body towards the achievement of the following governance outcomes: <ul style="list-style-type: none"> - Ethical culture; - Good performance; - Effective control; and - Legitimacy. (IODSA, 2016: 11)
Governance champion	The Head of Department is the corporate governance champion. The accountability cannot be delegated , but this function may be delegated to an executive or senior manager responsible for driving corporate governance within the department.
Corporate governance of ICT	The system by which the current and future use of ICT is directed and controlled.

TERM	DEFINITION
	Corporate governance of ICT involves evaluating and directing ICT use to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation. (ISO/IEC 38500:2015)
Department	Means a national department, a national government component, the Office of the Premier, a provincial department, or a provincial government component.
DPSA	Department of Public Service and Administration
EXCO	Executive Management Committee (consists of executive management members of the department)
GITO	Government Information Technology Officer (Cabinet Memorandum 38(a) of 2000)
Head of Department	It means the incumbent of a post mentioned in Column 2 of Schedule 1, 2, or 3 of the Public Service Act, 1994, and includes any employee acting in such position.
Head of ICT	Refers to the person heading the ICT component/office and could be the GITO depending on the naming convention used in the department
ICT	Information and communication technology
ICT initiative	<p>Includes all ICT information systems and related information technology used to enable business/services.</p> <p>An ICT initiative refers to using information and application systems and technology to achieve business objectives to enable service delivery. In terms of planning, this refers to related existing and planned initiatives. This generic term relates to:</p> <ul style="list-style-type: none"> • Bespoke and off-the-shelf information and application systems; and • Technology infrastructure to host and provide an electronic communication platform. <p>The management of initiatives addresses all the elements of the full lifecycle of ICT.</p>
IEC	International Electrotechnical Commission
Institutionalisation	Embed corporate governance of ICT as a custom or norm within the department or culture
ISO	International Organization for Standardization
ISO/IEC 38500:2015	An international standard for corporate governance of IT published jointly by ISO and the IEC
IT	Information technology
IT Service Management	A set of policies and practices for implementing, delivering, and managing IT services for end-users in

TERM	DEFINITION
	a way that meets the stated needs of end-users and the stated goals of the business (IBM, 2020)
Key driver	<p>A key driver is an activity in the performance value chain of the department.</p> <p>Within the context of the implementation of the corporate governance of the ICT system, key drivers are those leading factors or processes that affect the downstream activities or conditions. It provides for metrics to monitor implementation progress and performance.</p>
King IV	Report on Corporate Governance for South Africa, 2016
MPSA	Minister of Public Service and Administration
MTEF	Medium-Term Expenditure Framework
PFMA	Public Finance Management Act, 1999 (Act No. 1 of 1999)
Policy Framework	This Public Service Corporate Governance of ICT Policy Framework (CGICTPF)
Regime	A set of rules or a system or an ordered way of doing things that regulate the operation or way of doing things within the department
Responsible	Refers to the person who must ensure that activities are completed successfully
Responsible, Accountable, Consulted, Informed (RACI) chart	A diagram that identifies users' key roles and responsibilities against major tasks within a project (Software Advice, 2020)
Risk appetite	The amount of residual risk that the department is willing to accept (PSRMF 2010:15)
Risk management	A systematic and formalised process to identify, assess, manage and monitor risks (PSRMF 2010:16)

1. PURPOSE

The purpose of this Policy Framework is to institutionalise the corporate governance of ICT as an integral part of the corporate governance practices within departments in a uniform and coordinated manner.

Corporate governance of ICT will create value for the department, e.g., improved service delivery, better use of limited resources, and improved performance and quality. It will also provide for performance measurement of ICT as a strategic enabler of the department business, thus driving their respective digital transformation strategies.

The Policy Framework directs the **strategic leadership** of the department to take responsibility for the corporate governance of ICT and provide leadership for the use of ICT to support the achievement of the strategic objectives and goals of the department.

2. SCOPE

This Policy Framework for the corporate governance of ICT is applicable to all departments in the public service, as defined in section 197(1) of the Constitution of the Republic of South Africa, 1996, and section 7 of the Public Service Act, 1994 (Proclamation No. 103 of 1994), namely:

- National departments;
- Provincial departments;
- National government components; and
- Provincial government components.

3. REGULATORY FRAMEWORK

All the relevant acts and prescripts that regulate the strategic planning and corporate governance of the department are applicable to the ICT environment, such as:

- Constitution of the Republic of South Africa, 1996, section 197(1);
- Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
- Protection of Personal Information Act, 2013 (Act No. 4 of 2013).
- Public Administration Management Act, 2014 (Act No. 11 of 2014), section 14;
- Public Finance Management Act, 1999 (Act No. 1 of 1999);
- Public Service Act, 1994 (Proclamation No. 103 of 1994);
- Public Service Regulations, 2016; and
- Any other legislation applicable to the department.

4. APPLICABILITY

As departments differ in purpose, function, complexity, and size (*culture, goals, risks, compliance requirements, etc.*), there is no one-size-fits-all solution. This Policy Framework recognises this diversity. It is thus not possible to produce a blueprint of an enabling environment applicable to all departments.

This Policy Framework provides explanatory principles, practices, and the governance system to support and sustain effective departmental arrangements for using ICT in the public service.

5. BACKGROUND

In February 2013, the Minister of Public Service and Administration (MPSA), through Cabinet (Cabinet Memorandum No. 41 of 2012, dated 21 November 2012), issued the Public Service Corporate Governance of ICT Policy Framework and the related Corporate Governance of Information ICT Implementation Guideline and Corporate Governance of ICT Assessment Standard ("the Assessment Standard").

Since 2013, the introduction of the Policy Framework has improved awareness in the public service of the need for improved governance of ICT, as shown in several periodic assessment findings from the Department of Planning, Monitoring and Evaluation's (DPME's) Management Performance Assessment Tool (MPAT). This area's maturity levels (adoption and adaption) remain varied across the public service, as confirmed by the AGSA audit outcomes. For example, the recent 2020/21 financial year AGSA audit outcome still highlighted that 63% of auditees had weak IT governance practices, demonstrating a lack of accountability and oversight by those charged with overseeing IT performance and risk management.

Considering the above situation, combined with the compliance-focused approach of the 2012 approved Policy Framework, the need for a revised version became urgent and apparent.

6. INTRODUCTION

ICT has evolved and brings about new opportunities for the public service to expedite service delivery, reach citizens promptly, and promote two-way online communication between government and service beneficiaries. Furthermore, it provides public service senior management with the ability to make informed decisions based on easily accessible and reliable information.

To derive the expected value from the ICT investments, departments should strengthen ICT prescripts, ICT plans, ICT-enabled projects, and institutional arrangements. Therefore, executive management needs to incorporate ICT governance into existing corporate governance arrangements to oversee the performance of ICT.

7. OBJECTIVES OF POLICY FRAMEWORK

The objectives of this Policy Framework are to instil:

- (a) Executive management involvement and leadership in the governance of ICT within departments to create value and improve performance;
- (b) Transparency, accountability, and efficiency in matters related to the management of ICT; and
- (c) Enhanced level of ICT compliance and performance at a departmental level and in the public service.

8. BENEFITS OF CORPORATE GOVERNANCE OF ICT

When the corporate governance of ICT is effectively implemented and maintained, the following benefits, among other things, are to be realised:

- (a) Deriving business value from ICT investment;
- (b) Using, which includes sharing of departmental resources (*including but not limited to people, process, information and communication technology*) when investing in, operating and using ICT;
- (c) Mitigating ICT-related business risks of investing, owning, operating, and using ICT within a secure environment;
- (d) Improving ICT's ability to learn and the agility to adapt to changing circumstances; and
- (e) Improving ICT monitoring, evaluation, auditing, and reporting.

9. CORPORATE GOVERNANCE OF ICT IN THE PUBLIC SERVICE

9.1 Corporate governance

King IV defines corporate governance as the exercise of ethical and effective leadership by the governing body towards the achievements of the following governance outcomes:

- Ethical culture;
- Good performance;
- Effective control; and
- Legitimacy (IODSA, 2016).

When applied in the public service, corporate governance encompasses the mechanisms by which departments and those in leadership are held to account, the

risk is monitored and assessed, and performance is optimised.

It provides an appropriate control environment that enables strategic leadership and management to discharge their responsibilities and oversee compliance with legislation and prescripts.

9.2 Corporate governance of ICT

Corporate Governance of ICT involves evaluating and directing ICT use to support the organisation and monitoring this use to achieve plans (ISO/IEC 38500:2015).

Corporate governance of ICT is a subset of the department's corporate governance system (also called departmental arrangements) and consists of principles and practices within a system that enables strategic leadership to execute their oversight roles and responsibilities.

King IV code, Principle 12 states: “The governing body should manage technology and information in a way that supports the organisation in setting and achieving its strategic objectives” (IoDSA, 2016).

COBIT 2019 resonates with the King Code’s provisions. It highlights that the boards must exercise oversight to “enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from I&T-enabled business investments” (ISACA, 2018).

Because information is a critical asset in any organisation, its management, including the associated technological channels, requires the attention of decision-makers to ensure that information assets are utilised for the intended purposes. Therefore, decision-makers need to have appropriate governance oversight over technology that produces information and information itself. In view of departments' dependency on ICT for their successful existence and that ICT must be governed from the highest level of authority, corporate governance of ICT must be an integral part of the corporate governance system of departments. This approach will enable strategic leadership to execute their accountability and strategic leadership roles and responsibilities.

The corporate governance of ICT is implemented within the accountability structure of the department, as discussed in Section 11 of this Policy Framework.

10. LAYERED APPROACH TO CORPORATE GOVERNANCE OF ICT

Corporate governance of ICT encompasses two levels of decision-making, i.e.,

governance and management. There must be a clear distinction between these two layers, namely:

Corporate governance of ICT: the Executive Management Committee (EXCO) is accountable for achieving the department's mandate and strategic objectives through, among other things, the use of ICT. The accountability for corporate governance of ICT must be facilitated through clearly defined, implemented, and audited controls.

Management of ICT: the responsibilities and activities of ICT management and corporate governance of ICT differ.

ICT management entails a process whereby all operational activities concerning ICT resources are aligned to the department's priorities and needs. It includes tangible resources like networking hardware, computers, and people and intangible resources like software and data. The central aim of ICT management is to generate value through technology.

The ICT function is responsible for managing ICT processes that will ensure the effective and efficient execution and monitoring of ICT.

11. ACCOUNTABILITY STRUCTURE FOR CORPORATE GOVERNANCE OF ICT

Irrespective of the type of department, be it a national or provincial department, the corporate governance of ICT accountability structure provides for the roles and responsibilities of the different levels of corporate governance.

11.1 Governance structures

11.1.1 EXCO

The structure that has the highest level of accountability for the governance and performance of a department must provide monitoring and oversight to ensure that the use of ICT supports the achievement of the department's strategic objectives.

This governance structure must ensure that corporate governance of ICT is included in the corporate governance regime of the department and that the necessary governance structures, policies, and processes are in place, monitored, and enforced.

In addition to other EXCO roles and responsibilities, this structure Evaluate, Direct and Monitor the effectiveness of the departmental ICT governance system, including but not limited to:

- Approve CGICT Policy, ICT plan (MTEF), ICT operational plan, and other related plans and policies;
- Provide strategic direction to ICT by outlining the departmental strategic plan;
- Monitor that the ICT plan supports the department to deliver on its objectives per the strategic plan;
- Monitor and evaluate the performance of the ICT governance structures and processes;
- Approve portfolio of ICT projects and their related expenditure; and
- Oversee the implementation of the CGICT Policy Framework and associated policies and strategies.

11.1.2 ICT steering committee

Responsible for ensuring that departmental arrangements for the corporate governance of ICT are developed, implemented, managed, monitored, and evaluated. Furthermore, the ICT steering committee is responsible for creating an environment that improves the financial and performance management of ICT and managing ICT risks within the risk appetite of the department.

The ICT steering committee is responsible for:

- Providing oversight on the management and use of ICT in the department;
- Providing strategic leadership towards the digitalization of the department, including ICT projects and services;
- Monitoring the joint ICT planning and resourcing of the ICT programme across the department;
- Monitoring the implementation of approved plans, policies, strategies;
- Monitoring that ICT related business risks are mitigated, benefits realization from the ICT investments (portfolio of ICT projects), and audit issues from assurance providers; and
- Providing recommendations and reporting to EXCO on pertinent ICT issues, including ICT strategies and plans.

The ICT steering committee must operate as a project steering committee where

no separate committee exists.

11.2 Roles and Responsibilities

11.2.1 Head of Department

Provides strategic leadership to ensure efficient and effective use of ICT within the department as contemplated in regulation 30 of the Public Service Regulations, 2016. The Head of Department is responsible for creating an environment that helps improve the department's financial and performance management.

The Head of Department is the **designated governance champion** accountable for the corporate governance of ICT and is responsible for the establishment of corporate governance of the ICT system and monitoring of its performance. The corporate governance champion responsibility may be delegated to a person on a senior management level with the authority to establish and monitor the corporate governance of the ICT system across the different business units.

However, accountability for the performance of the corporate governance of the ICT system shall remain with the governance champion.

It is recommended that the responsibilities of the governance champion include the following:

- (a) Overseeing that the corporate governance of ICT system, as a subset of Corporate Governance, is developed, implemented, maintained, reported on, and change management effected; and
- (b) Being actively involved in the oversight of the formal corporate governance system of the department.

The governance champion must be supported by a cross-functional team that must include business and ICT.

11.2.2 Head of ICT

Responsible for aligning the use of ICT, as a strategic resource, with the business requirements in fulfilling its strategic mandate within a secure information environment. Other responsibilities include:

- Overseeing and directing the day-to-day activities of the departmental ICT

department, ensuring that systems, services, and infrastructure work reliably and securely, and

- Participation in developing the digital transformation strategy focusing on the department's optimization and transformation of ICT.

The Head of ICT must manage the ICT function through a defined IT Service Management policy.

The Head of ICT must attend EXCO meetings. In these meetings, the Head of ICT must identify and implement possible solutions for ICT use to achieve the department's objectives.

Although this Policy Framework does not address the management of ICT aspects in detail, the Head of ICT will be responsible for providing a regular executive summary to the ICT steering committee and EXCO on the following key general IT controls:

- Information security management;
- User access management;
- ICT service continuity;
- Management of external service providers (3rd parties); and
- Configuration management (IT assets lifecycle management).

In addition, the Head of ICT is responsible for reporting to EXCO on key ICT operational matters that potentially impact the achievement of departmental objectives through the implementation of ICT-enabled projects.

12. POLICY FRAMEWORK FOR CORPORATE GOVERNANCE OF ICT IN THE PUBLIC SERVICE

This Policy Framework provides for the following:

1. **Principles** are rules (compulsory to comply with) that guide decision-making and behaviour. These principles establish the context for effective, efficient, and

acceptable use of ICT. The principles guiding corporate governance of ICT in the public service are given in Section 13 of this Policy Framework.

2. **Practices** are specific actions that prescribe how and by whom the principles will be implemented. The practices that are in support of the principles are given in Section 13 of this Policy Framework.
3. A **system** is a set of means and mechanisms that enable the implementation of corporate governance of ICT. In this system, executive and strategic leadership are primary to sustained corporate governance of ICT. The system explains how the ICT effort of a department is governed through the governance tasks of evaluating, directing, and monitoring. The system to implement corporate governance of ICT is discussed in Section 14 of this Policy Framework.

The principles and practices are implemented within an accountability structure in the department, as discussed in the following section.

13. PRINCIPLES AND PRACTICES

This Policy Framework is based on priorities stated in the National Development Plan 2030, the Public Service Act, 1994, the Public Service Regulations, 2016, and the Public Administration Management Act, 2014. It is underpinned by concepts, such as principles, practices, and a system, from the King IV Code of Governance for South Africa (2016) and the International Organization for Standardization's ISO/IEC 38500:2015.

Table 1 below contains the principles that are compulsory to comply with and explains the practices that should be adapted and adopted to suit the unique context and ecosystem of the department.

Table 1: Corporate governance of ICT principles and practices

<p>Principle 1: Strategic mandate</p> <p><i>ICT (current and future capabilities) must enable the department to achieve its strategic mandate and objectives.</i></p>
<p>Practices:</p> <p>As contemplated in regulation 93 of the Public Service Regulations (PSR), 2016, the head of department shall ensure that the acquisition management, and use of</p>

information and communication technologies by the department enhances direct or indirect service delivery to the public, including but not limited to equal access by the public to services delivered by the department. The PSR further provides for the head of department to ensure that such acquisition, management, and use of information and communication technologies improve the department's productivity. In terms of governance of ICT, this shall include:

- 1.1 Ensuring that corporate governance of ICT is included in the strategic leadership and oversight responsibility of the department to achieve the strategic objectives of the department;
- 1.2 Providing strategic structural requirements of the ICT function to provide adequate capacity and capability for the use of ICT to enable business; and
- 1.3 Ensuring that ICT planning methodology and instruments are aligned with the business requirements.

Principle 2: Institutionalisation of corporate governance of ICT

Corporate governance of ICT must be institutionalised within the corporate governance regime of the department.

Practices:

- 2.1 Ensuring that corporate governance of ICT is embedded in the corporate governance regime of the department; and
- 2.2 Providing oversight to ensure that effective ICT prescripts, structures, strategic plans, and corporate governance of the ICT system (see Section 14) are institutionalised to evaluate, direct, and monitor ICT use.

Principle 3: Value and benefit realisation from ICT investment

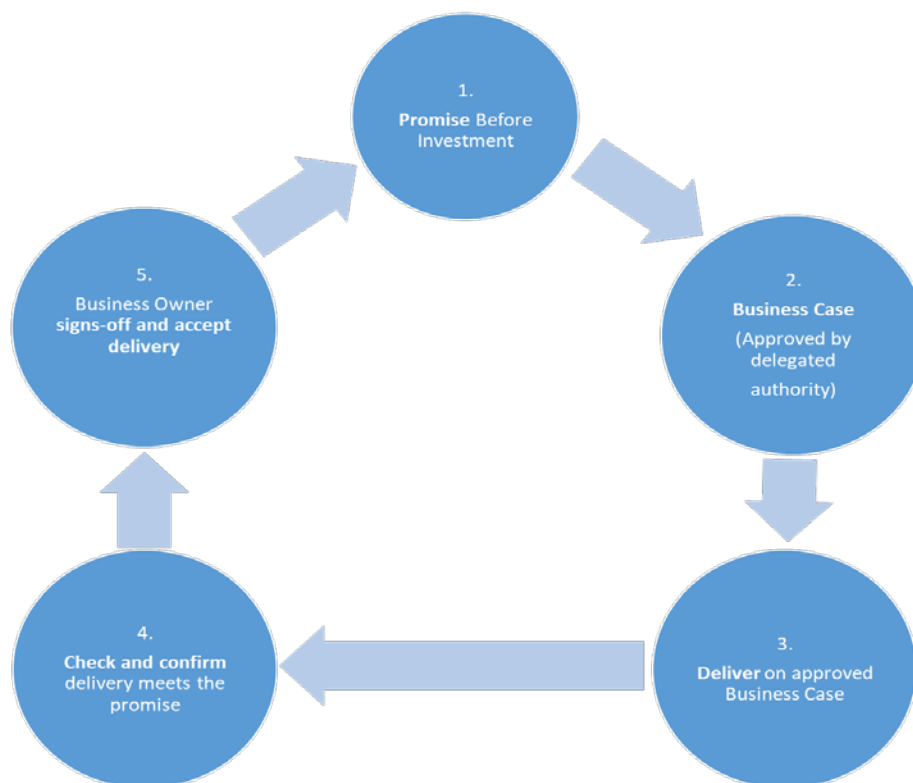
All ICT investments must achieve the predetermined value and benefits.

Practices:

As contemplated in section 38(a)(iii)(b) of the Public Financial Management Act (PFMA), 1999, the accounting officer must ensure that the department has and maintains an appropriate procurement and provision system which is fair, equitable, transparent, competitive and cost-effective. The PFMA further provides for the accounting officer to ensure that the department has and maintains effective, efficient,

economical, and transparent use of the department's resources. In terms of governance of ICT, this shall include:

- 3.1 Ensuring that responsible ICT investment practices are in place to promote good governance and the creation of value and benefits;
- 3.2 Determining upfront the expected benefits and value from an ICT investment;
- 3.3 Oversee the value and benefits delivered through these major ICT investments and significant ICT operational expenditure;
- 3.4 Concurrence of the Head of ICT in all ICT related decisions, including procurement; and
- 3.5 Ensuring that an executive manager responsible for the ICT initiative/project signs off, confirming value realization as per the figure below.



Principle 4: Manage ICT-related business risks

The ICT-related business risks, including security and cybersecurity, must be managed (mitigated and audited regularly).

Practices:

As contemplated in section 38(a)(i) of the PFMA, the accounting officer must ensure that the department has and maintains effective, efficient, and transparent financial and risk management and internal control systems. In terms of governance of ICT, this shall include:

- 4.1 Ensuring that ICT related business risks (including cybersecurity) are addressed as part of the risk and audit regime of the department; and
- 4.2 Overseeing that financial and other risks of major ICT investments are managed.

Principle 5: Change management/departmental behaviour

Corporate governance of ICT must be implemented through appropriate change management interventions.

Practices:

- 5.1 Setting the example to adopt and influence culture change within the department (lead by example);
- 5.2 Direct and oversee that culture change of departmental behaviour is effected through change management; and
- 5.3 Support and be early adopters of change initiatives.

Principle 6: Monitoring and evaluation (This principle cuts across all the other principles and practices)

Monitor and evaluate the use and performance of ICT.

Practices:

As contemplated in regulation 9(2) of the PSR, the head of department shall introduce mechanisms to monitor and evaluate any provision of the Public Service Act, 1994. In terms of governance of ICT, this shall include:

- 6.1 Providing oversight to ensure that the principles and practices are

- implemented, monitored, and evaluated to ensure the governance mechanisms remain functional and effective;
- 6.2 Overseeing compliance with regulatory prescripts, policies, and standards that have an impact on the performance of ICT; and
- 6.3 Overseeing performance against targets and objectives (benefits realisation, alignment with business goals, risk management, and resource optimisation).

14. CORPORATE GOVERNANCE OF ICT SYSTEM

This Policy Framework will be institutionalised through corporate governance of the ICT system, which explains the relationship between governance, strategic leadership, and management and their associated responsibilities.

The corporate governance of the ICT system is the system by which the current and future use of ICT resources is directed and controlled to facilitate the achievement of the department’s strategic objectives. It refers to all the means and mechanisms that enable the department’s EXCO, Head of Department, and ICT steering committee to provide direction and oversight.

The system mentions the corporate governance tasks of evaluating, directing, and monitoring used to apply the principles and practices, as explained in Section 13.

The functioning of the corporate governance of the ICT system is depicted in **Figure 1** below.



Figure 1: Corporate governance of the ICT system

(Adapted from ISO/IEC 38500: 2015(a))

- At the core of the corporate governance of the ICT system are leadership, structures, prescripts, and procedures to evaluate, direct and monitor the efficient and effective use of ICT to achieve the strategic mandate and objectives of the department, appropriate management of risks and responsible use of resources. It includes determining the alignment between business requirements and ICT plans;
- Through these governance tasks, stakeholder needs and options are evaluated to determine the departmental objectives. Direction is provided through prioritisation of proposals/options, and decision-making and monitoring are done by measuring performance and compliance against agreed-on direction and objectives;
- EXCO, which is accountable, provides the strategic direction of the department. The strategic direction and the external and internal context determine the strategic objectives. The management of business execution is done through the organisational structure and use of the relevant resources;
- The different accountability structures must monitor, evaluate and report on the execution of these initiatives to ensure that the desired outcomes are achieved within the prescriptive and a secure environment; and
- All the ICT-related initiatives, such as regulatory prescripts, standards, and transversal initiatives, which impact ICT performance, must be reviewed regularly.

15. IMPLEMENTATION OF A CORPORATE GOVERNANCE OF THE ICT SYSTEM

Corporate governance of the ICT environment is established by developing and implementing means and mechanisms such as strategies, structures, policies, frameworks, procedures, plans, controls, change management, and ethical culture. (A minimum enabling environment must be created through these means and mechanisms.)

Departments must adopt the Policy Framework and adapt it to suit their unique context and ecosystem and **explain** how their system sustains the principles and practices.

- The **principles** (rules) must specify the preferred behaviour that will guide decision-making.
- The **practices** (actions) must explain how and by whom these principles will be implemented within the department.
- The **system** (means and mechanisms) must enable the department's EXCO, Head of Department, and ICT steering committee to provide direction and oversight

The departmental corporate governance of ICT arrangements **must** show:

- (a) The **scope** and **regulatory requirements** applicable to corporate governance of ICT as applied to the specific department;
- (b) The departmental interpretation of how the corporate governance of ICT **objectives** will be applied;
- (c) How the ICT strategic objectives will be **aligned** with departmental strategic objectives, **monitored**, and **reported** on to the relevant stakeholders to create value through the use of ICT;
- (d) The departmental interpretation of how the **principles and practices** will be applied;
- (e) How the **system** of corporate governance of ICT will be implemented within the department; and
- (f) How the departmental corporate governance of ICT will be maintained.

Departments must clearly indicate their related structures and procedures and the accountability and responsibilities that are allocated to each. This responsibility assignment can be reflected in a responsibility, accountability, consultation, and information (RACI) chart.

Existing structures can be used to perform these functions.

15.1 Business enabling policies, frameworks, and plans

To enable the performance of ICT, specific business-related policies and/or frameworks are required, e.g.:

- (a) **Departmental corporate governance of ICT policy** – departments must develop departmental corporate governance of ICT policy in line with a DPSA

policy template. This policy must provide explanatory principles, practices, and corporate governance of the ICT system to support and sustain effective departmental arrangements for ICT use within the department.

(b) **Information security policy** – departments must develop an information security policy, which is an overarching policy, including cybersecurity, and related sub-policies such as:

- access management;
- incident management;
- problem management; and
- change management (including patch management).

These ICT security prescripts must indicate how the department will manage the protection of electronic information, related systems, and infrastructure.

(c) **ICT service continuity plan** – departments must develop an ICT continuity plan aligned with and informed by the departmental business continuity plan, which is the responsibility of Enterprise Risk Management.

(d) **ICT project management framework** – departments must adopt and develop a project management framework to manage ICT initiatives. ICT projects should be embedded in the departmental portfolio, programme, or project management structures to ensure ICT project oversight.

At a minimum, the Framework must address the following deliverables:

- Project Governance (roles and responsibilities);
- Project Conceptualisation;
- Project Prioritization;
- Project Initiation;
- Project Planning;
- Project Execution;
- Project monitoring and control;
- Quality Management; and
- Risk Management.

All investments for the business enabling ICT projects and ICT operational projects exceeding R10 million rands or projects cutting across government must have an approved business case.

- (e) **ICT end-user policy (acceptable use)** – departments must develop a policy to ensure proper use of departmental ICT assets. The policy must apply to any ICT asset the department has or may install in the future, including but not limited to email, Internet, mobile data cards, and desktop computing.
- (f) **IT service management policy** – departments must develop a policy defining the implementation and management of quality ICT services that meet the business needs. This policy must serve as the ICT function commitment to serve the business.

At a minimum, the policy must address the IT Service Lifecycle Management, highlighting the following aspects:

- Service Level Management (service catalog, service requests, and turnaround times or service targets);
- Availability management (availability plan);
- Demand management (capacity versus demand);
- ICT financial management (costs, charges, and budget);
- Supplier Management (management of external service providers); and
- Configuration management (IT assets lifecycle management).

16. ICT ALIGNMENT PLANNING

Departments must use ICT as a strategic resource to create value by enabling its strategic mandate and objectives. To achieve this, departments should plan over the long, medium, and short term for ICT to enable the business and create value for the department.

ICT planning must follow the relevant planning prescripts, methodology, and planning periods. This planning practice culminates in the following plans:

- (a) **Departmental strategic plan** – departments must indicate how ICT will be used to support the achievement of the departmental targets and objectives

as contemplated in regulation 25 of the Public Service Regulations, 2016.

- (b) **ICT plan (three-year plan)** – departments must develop and maintain an ICT plan aligned to the medium-term expenditure framework for the department. This plan must address the people, processes, and technology matters to achieve departmental objectives as contemplated in regulations 25 and 38 of the Public Service Regulations, 2016.
- (c) **ICT operational plan (one-year plan)** – departments must develop and maintain an ICT operational plan that reflects the current year's implementation and monitoring of ICT initiatives and projects.

17. MONITORING AND EVALUATION

The implementation of the Policy Framework is measured through the Assessment Standard and/or other related standards.

- (a) The Assessment Standard will measure the **compliance** with the Policy Framework and the **performance** of the ICT function to enable the achievement of business objectives and value creation for the department. The Assessment Standard includes a balanced scorecard with guiding criteria to assess the compliance and performance of ICT.
- (b) This Assessment Standard will provide departments with self-assessment criteria to measure ICT compliance and performance.
- (c) The Assessment Standard will also be used by the Department of Public Service and Administration (DPSA) to measure performance and compliance with the corporate governance of ICT standards.

18. GOVERNMENT-WIDE ICT PROJECT GOVERNANCE MECHANISM

The AGSA data shows that the individual departmental intervention plans to address the recurring AGSA findings on Information Systems audits are not yielding the expected results. As a result, the government urgently requires a government-wide ICT project governance mechanism to provide quality assurance on significant ICT projects impacting several departments. This mechanism will ensure that no large-scale project is managed on a standalone basis and provides oversight on significant investment projects. The details of this mechanism will be dealt with separately.

19. NON-COMPLIANCE

Failure to comply with this Policy Framework will be dealt with in line with the provisions of the Public Service Act, 1994, sections 16A and 16B.

20. CONCLUSION

Implementing this Policy Framework promotes efficient and effective ICT governance for the departments to achieve their strategic objectives through the governing tasks of evaluating, directing, and monitoring.

Departments must apply corporate governance of ICT by adopting the principles and practices put forward in this Policy Framework (comply with) and adapting their governance system to align with their departmental context (explain) while keeping the intent of this Policy Framework intact.

The Assessment Standard will be based on a balanced scorecard for implementing corporate governance of ICT for both compliance measurement **and performance measurement levels.**

This Policy Framework must be institutionalised through corporate governance of the ICT system, which guides the relationship between governance and management and their associated responsibilities.

This Policy Framework serves as the foundation for the corporate governance of ICT in the public service. Changes or enhancements to this policy will be dealt with through directives and determinations addressing specific subjects

21. REFERENCES

- (1) Auditor-General of South Africa. (2019). *2018-19 PFMA Consolidated general report on national and provincial audit outcomes*. Pretoria: Office of the Auditor-General of South Africa.
- (2) Department of Finance. (2010a). *Public Sector Risk Management Framework*. Published 1 April 2010. Pretoria: National Treasury.
- (3) Department of Public Service and Administration. (2000a). *Cabinet Memorandum 38a of 2000*. Pretoria: Department of Public Service and Administration.
- (4) Department of Public Service and Administration. (2006). *Batho Pele Handbook*. Pretoria: Department of Public Service and Administration.
- (5) Department of Public Service and Administration. (2012). *Public Service Corporate Governance of Information and Communication Technology Policy Framework*. Cabinet Memorandum 41 of 2012. Pretoria (Gauteng): Department of Public Service and Administration.
- (6) Department of Public Service and Administration. (2014a). *Public Administration Management Act, 2014 (Act No. 11 of 2014)*. Cape Town: Government Printing Works.
- (7) IBM. (2020). IT Service Management (ITSM). IBM Cloud Education Retrieved from <https://www.ibm.com/za-en/cloud/learn/it-service-management> [Accessed 24 November 2021].
- (8) Information Regulator of South Africa (2000). Promotion of Access to Information Act, 2000 (Act No. 2 of 2000). <https://www.justice.gov.za/infoereg/docs.html> [Accessed 17 December 2020]
- (9) Information Regulator of South Africa (2013). Protection of Personal Information Act, 2013 (Act No. 4 of 2013). <https://www.justice.gov.za/infoereg/docs.html> [Accessed 17 December 2020]
- (10) Institute of Directors in Southern Africa. (2016). *King IV Report on Corporate Governance for South Africa 2016*. Johannesburg: Institute of Directors in Southern Africa.
- (11) International Organization for Standardization. (2014). *ISO/IEC TR 38502 Information Technology - Corporate Governance of ICT - Framework and model*. Geneva (Switzerland): ISO.

- (12) International Organization for Standardization. (2015a). *ISO/IEC 38500 Information technology - Governance of IT for the organization*. 2nd ed. Geneva (Switzerland).
- (13) International Organization for Standardization. (2015b). *ISO/IEC TS 38501 Information technology - Governance of IT - Implementation Guide*. 1st ed. Geneva: ISO.
- (14) International Standards Organization. (2014). *ISO/IEC TR 38502 Information Technology - Corporate Governance of IT – Framework and model*. 1st ed. Switzerland.
- (15) ISACA (2018). *COBIT 2019 Implementation Guide – Implementing and Optimizing Information and Technology Governance Solution*. Retrieved from <https://www.isaca.org/COBIT/Pages/COBIT-2019-Implementation-Guide.aspx>. [Accessed 19 April 2019].
- (16) Kaplan, R.S. and Norton, D.P. (1996). *Linking the Balanced Scorecard to Strategy*. California Management Review. Volume 39, No. 1. Available at <http://www.strategyinstitute.co.za/PDF/bsc.pdf>. [Accessed 19 March 2018].
- (17) National Treasury. (2010b). *Framework for Strategic Plans and Annual Performance Plan*. August 2010. Pretoria: National Treasury.
- (18) Software Advice. (2020). *What Is a RACI Chart? Here's Everything You Need To Know*. Retrieved from <https://www.softwareadvice.com/resources/what-is-a-raci-chart/>. . [Accessed 24 November 2021].
- (19) The National Computing Centre. (2005). *IT Governance Developing a successful governance strategy. A Best Practice guide for decision-makers in IT*. www.ncc.co.uk.
- (20) The Presidency. (2005). *Intergovernmental Relations Framework Act, 2005 (Act No. 13 of 2005)*. 15 August 2005. The Presidency. Cape Town: Government Printing Works.
- (21) The Presidency. (2007). *Policy Framework for the Government-wide Monitoring and Evaluation System*. November 2007. Pretoria: The Presidency.