

ANNEXURE A: Information and Communication Technology (ICT) Risk Management Toolkit

INFORMATION AND COMMUNICATION TECHNOLOGY RISK MANAGEMENT TOOLKIT

Version 1
(August 2023)

TABLE OF CONTENTS (ICT Risk Management Toolkit)

Contents	Page
1. Introduction.....	34
2. Purpose.....	34
3. Scope and Applicability.....	35
4. Risk Management in the ICT Context.....	35
5. ICT Risk Categories.....	36
6. The ICT Risk Management Process.....	45
7. Conclusion.....	45
8. Approval of the ICT Risk Management Toolkit and Date of Effect.....	44

1. Introduction

- 1.1 In the context of the current democratic dispensation, the South African citizens are stakeholders of the Public Service as an institution.
- 1.2 The activities, operations and projects of the DR&PW as a provincial institution of the Public Service have inherent uncertainties and opportunities, thus making the attainment of objectives for service delivery to stakeholders challenging in some respects.
- 1.3 The nature of Information and Communication Technology (ICT) risks tend to differ from one scenario to another, as well as from one organization to the other. Despite that, all ICT risks can generically be mapped down to inadequate and/or poor governance of enterprise Information Technology (IT).
- 1.4 This ICT Risk Management Toolkit seeks to outline and simplify the most common risk scenarios that the DR&PW have to cater for before, during and after the acquisition/development of an ICT solution and/or system.
- 1.5 For the public service, and thus also for the DR&PW, the Executive Management is accountable for Risk Management. However, it is important to emphasize that every employee in an organization has responsibility for risk management and in this case specifically also for ICT risk management.
- 1.6 This then calls for risk management and specifically also ICT risk management to be fully integrated into the daily business and service delivery operations of the Department.

2. Purpose

- 2.1 The purpose of this ICT Risk Management Toolkit is to:
 - a) promote risk aware behaviour in the DR&PW when acquiring, developing and managing ICT systems and/or solutions;
 - b) constantly focus on the DR&PW's service delivery objectives when investing and/or using ICT and related services;
 - c) make ICT Risk Management part of the departmental management and decision making processes;
 - d) provide a systematic and logical approach to be followed by the DR&PW when proactively and reactively managing ICT risks;

- e) make departmental staff aware of risks associated with the usage of ICT and promote responsible risk taking when using various applicable ICT systems, platforms, programmes, applications, etc.; and
- f) increase the chances of success for all departmental ICT, related activities or initiatives and the management thereof.

3. Scope and Applicability

- 3.1 This ICT Risk Management Toolkit complements the DR&PW's policies, strategies and plans regarding risk management and the Public Service Wide Enterprise Risk Management (ERM) Framework issued by the National Treasury provides the framework for its methodology.
- 3.2 This Toolkit shall therefore be applied within the context of the above-mentioned departmental and national frameworks, as well as the DR&PW's specific goals and objectives.
- 3.3 This Toolkit assumes that the DR&PW have determined the Risk Appetite and Risk Tolerance levels relevant for the departmental ICT environment. Consequently, the use of this Toolkit will also be influenced by such determinations within the Department.
- 3.4 Finally, this Toolkit shall be applicable when acquiring, developing and/or using ICT systems and/or solutions as a means to attain the DR&PW's objectives, including in daily operations.

4. Risk Management in the ICT Context

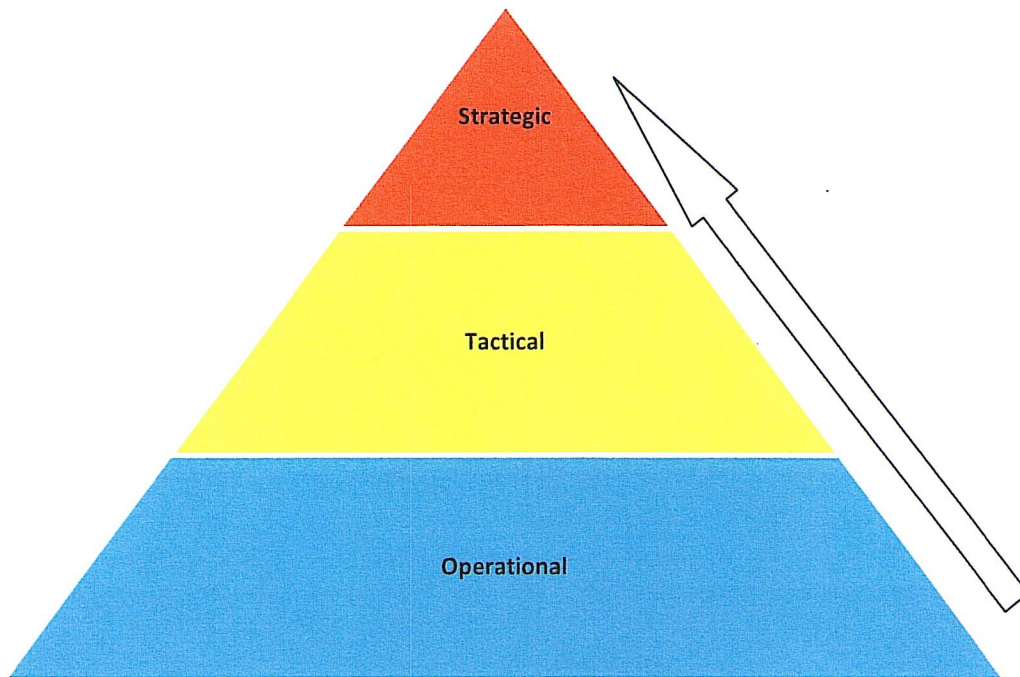
- 4.1 In line with the International Standards Organization (ISO 31010: 2009) and the South African National Standards (SANS 31010: 2010) for the Public Service, an ICT risk shall be defined as ***'the effect of uncertainty on objectives'***.
- 4.2 ICT risks would therefore refer to uncertainty in achieving the DR&PW's ICT objectives. This definition recognizes that organizations generally exist and operate under uncertain circumstances.
- 4.3 Given such uncertainty, there is always a chance for deviation in the achievement of organizational objectives and goals versus the plans and expectations. While deviation may be positive or negative, such deviation must be actively managed in order to achieve the departmental goals and objectives, in line with approved plans and expectations.

- 4.4 Therefore, ICT Risk Management shall be defined as the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects that the DR&PW faces as it seeks to achieve its ICT and related service delivery objectives.
- 4.5 It is important to emphasize that risks in the Department can only occur within the context of particular objectives, be it finance, security, human resources, or information technology and can also be related to other functional areas of the DR&PW.

5. ICT Risk Categories

- 5.1 There are various ways to categorize risks, including within the ICT environment. Risks could be categorized as being strategic, tactical or operational in nature. Risks can also be related to markets (market risks), legislation (compliance risk), the environment (environmental risks), politics (political risks, etc).
- 5.2 For purposes of this Toolkit, a Strategic Risk refers to uncertainty in the achievement of the Department's high level and long term (strategic) goals. Generally, a strategic risk impacts an organization at a strategic level (Executive Management level).
- 5.3 On the other hand, a Tactical Risk refers to uncertainty in the achievement of the Department's service delivery goals and objectives, mainly due to the approach adopted when trying to achieve them. Generally, a tactical risk impacts an organization at a Unit or Directorate level.
- 5.4 An Operational Risk refers to uncertainty in the achievement of the Department's service delivery goals and objectives due to inadequacy, ineffectiveness or failure of systems, controls, people, and/or processes within the DR&PW.

Figure 1: ICT Risk Categories

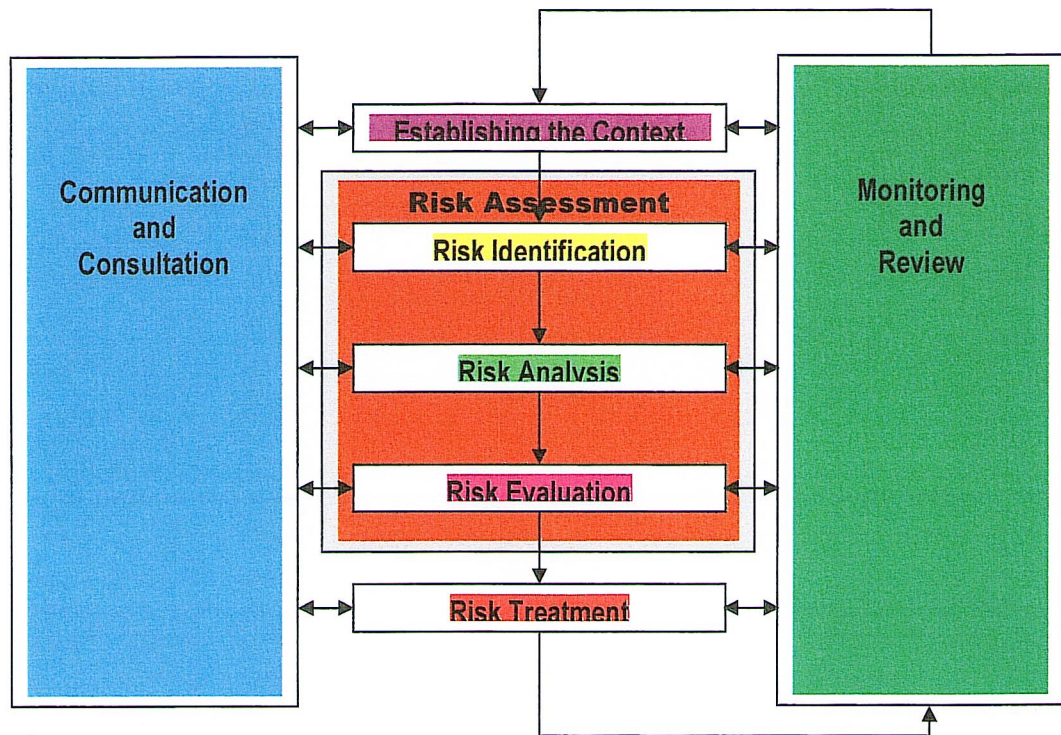


- 5.5 It is also vital to highlight that uncertainty in the achievement of departmental objectives is always brought about by factors either internal or external to the DR&PW, or activity under scrutiny. It is further important to highlight that a risk can impact an organization at more than one level.
- 5.6 In addition to this Toolkit being applicable to various categories of ICT risks identified above, below is the generic risk management process that shall be applicable when managing ICT risks in the DR&PW.

6. The ICT Risk Management Process

- 6.1 The ICT Risk Management Process comprises of key sub-processes and/or activities performed by the Department towards the management of ICT risks. These are communication and consultation, establishing context, risk assessment, risk treatment as well as monitoring and review.
- 6.2 While the communication and consultation sub-processes emphasize the need for constant interaction and/or communication amongst all relevant stakeholders during the ICT risk management process, establishing the context emphasizes the need for the ICT risk management process and the Risk Owners to understand both the internal and external environments within which the Department exists and hence risk occurs.
- 6.3 While the internal environment would focus on the organizational objectives, processes and capabilities, the external environment focuses on political, economic, social, technological, environmental and legal (PESTEL) factors impacting on the DR&PW.
- 6.4 The risk assessment sub-process focuses on the identification, analysis and evaluation of ICT risks, while the risk treatment sub-process focuses on selection and agreement amongst stakeholders, on one or more options to implement in order to reduce and/or totally eliminate uncertainty towards the achievement of departmental objectives.
- 6.5 The monitoring and review sub-process focuses on continuously evaluating the implemented ICT risk controls in order to ascertain whether they have achieved the expected results, with a view to modify such controls if they are found to be ineffective.

Diagram 2: The ICT Risk Management Process



- 6.6 Guided by the generic management process and/or methodology highlighted above, this ICT Risk Management Toolkit shall be utilized when managing ICT risks within the Department.
- 6.7 Firstly, an ICT risks rating shall be performed before, during and after a solution is acquired and/or developed. Rating risk scenarios before and during the solution acquisition and/or development process shall serve to set the recommended ICT Risk Appetite and ICT Risk Tolerance levels associated with the solution, while risk rating after the solution development shall serve to indicate the level of ICT Risk Exposure by the Department.
- 6.8 In rating ICT risks, a scale of Non Compliant (NC), Partially Compliant (PC), Largely Compliant (LC), Compliant (C) and Not Applicable (N/A) shall be used. In addition, the level of compliance of each evaluation process shall be calculated and be allocated a compliance rating using a percentage point. For example, if 10 out of 25 Risk Focus Areas are C and/or LC to ICT policies, standards and practices, the risk rating for such a solution (whether proposed/ acquired/ developed) shall be 40%.
- 6.9 The Department should then take appropriate action given such percentage risk rating score. It is worth mentioning that these ratings are self explanatory as, for instance, a non compliant (NC) risk

rating indicates that an ICT solution, activity or process does not comply with public service ICT policies, standards and specified key best practices in the ICT environment.

6.10 Below are the various **ICT Risk Focus Areas** to be evaluated during the ICT Risk Assessment process.

Table 4: ICT Risk Focus Areas

ICT RISK FOCUS AREA	DESCRIPTION	RISK RATING: C/LC/PC/NC/NA
1. Strategy	This risk focus area evaluates the extent to which the acquired/developed ICT solution/system is aligned to the Department's business and ICT strategy.	
2. Legal and Regulatory Compliance	This risk focus area evaluates the extent of compliance to Laws and Regulations governing the service in question as well as ICT in the public service.	
3. Intellectual Property Rights (IPR)	This risk focus area evaluates the IPR ownership and related issues pertaining to the acquired/developed ICT solution/system.	
4. Internal Governance	This risk focus area evaluates the extent, to which the departmental governance structures, policies, systems, principles, processes (<i>including business case and decision making processes</i>) and controls have been adhered to or followed during the acquisition and or development of the ICT solution/system under consideration.	
5. Client Convenience	This risk focus area evaluates the extent to which the acquired/developed ICT solution/system brings about convenience to the clients.	
6. Economies of Scale	The focus area evaluates the extent to which the	

	acquired/developed ICT solution/system can be applicable and/or utilized in addressing other related and/or similar departmental business challenges (<i>in other service delivery areas of the Department</i>) in addition to the initial reasoning/business case/rationale for acquiring/developing the particular ICT solution/system.	
7. Value for Money	This risk focus area evaluates the extent to which the acquired/developed ICT solution/system brings about efficiencies and effectiveness (<i>including service delivery efficiencies</i>) to the Department. The focus area further evaluates the extent to which the acquisition of a solution, against the purchase price and other ongoing costs (<i>including non-financial</i>), shall continuously remain justifiable.	
8. Lower Costs	This risk focus area evaluates the extent to which the acquired/ developed ICT solution/ system assist the Department/ public service in lowering costs (<i>financial</i>) of doing its business.	
9. Increased Productivity	This risk focus area evaluates the extent to which the acquired/developed ICT solution/system assist in increasing output productivity of the Department, including that of the employees.	
10. Eliminate Duplication	This risk focus area evaluates the extent to which attempts have been made to leverage or use other existing ICT solutions/systems within the Department, instead of acquiring and/or developing a new ICT solution/system.	
11. Digital Inclusion	This risk focus area evaluates the extent to which the proposed/acquired/developed ICT solution/system addresses equity and redress issues by ensuring that	

	more people have access to services.	
12. Portfolio and Project Management	This risk focus area evaluates the extent to which portfolio management practices have been adopted when acquiring the ICT solution/system. The focus area further evaluates the extent to which best practice project management methodology and practices (<i>Project Governance Issues</i>) have been followed during the ICT system/solution acquisition/development and implementation.	
13. Requirements Analysis	This risk focus area evaluates whether or not the documented and signed-off business requirements were provided and analysed before the ICT solution/system was acquired.	
14. Solution Design	This risk focus area evaluates the extent to which the proposed/acquired/ developed ICT solution/system has been designed and implemented to meet the documented business requirements thus ensuring the attainment of business objectives.	
15. Supplier Management	This risk focus area evaluates the extent to which policies, practices and processes have been put in place to ensure effective management of the supplier/service provider of the acquired ICT solution/system. The focus area looks at the contract/business agreement, service level agreement and other relevant protocols to support the agreement(s) between the Department and the solution/system supplier.	
16. Enterprise Architecture	This risk focus area evaluates the extent to which the acquired/developed ICT solution/system conforms/ complements the defined departmental Enterprise Architecture.	

17. Interoperability	This risk focus area evaluates the extent to which the acquired/developed ICT solution/system interoperates with other departmental/public service systems.	
18. Security	This risk focus area evaluates the extent to which the acquired/developed ICT solution/system presents physical, logical and other security issues and measures taken to address these issues. The focus area further evaluates data/information security/privacy issues associated with the acquired/developed ICT solution/ system and measures taken to mitigate against such issues.	
19. Business Process	This risk focus area evaluates the extent to which business processes to be supported by the acquired ICT solutions/systems are understood and have been documented. Optimisation of such processes is also the interest of this Risk Scenario/focus area.	
20. Problem and Incident Management	This risk focus area evaluates the system(s) and/or process(es) and/or procedure(s) to be followed and/or used to resolve problems, incidents and issues (<i>solution support</i>) related to the acquired/developed system from the time they occurred to their conclusion.	
21. Capacity Management	This risk focus area evaluates the extent to which the system capacity management requirements have been considered and catered for during the solution acquisition and/or development and implementation.	
22. Business Continuity	The focus area evaluates the alignment between the departmental business continuity requirements and ICT service continuity plans of the acquired and/or developed solution/system.	

23. Monitor, Evaluate and Assess Performance	This risk focus area evaluates the mechanisms and extent to which performance of the acquired ICT solution/system is monitored, assessed and reported to the relevant authority.	
24. Testing	This risk focus area evaluates the functional test cases provided and agreed upon with the departmental system owner/user and the supplier for the proposed/acquired/ developed ICT solution/system. This focus area further evaluates whether sufficient testing was done on the acquired/developed ICT solution/system (e.g. unit, integration, stress testing, end-to-end, etc.) before it is handed over to the Department.	
25. Relevant Documentation	This risk focus area evaluates whether all the necessary documentation, including but not limited to the Project Initiation Document, solution/ system design, solution/system configuration, project documentation, have been created and handed over to the Department before, during and after an ICT solution/ system is acquired/ developed.	
26. Organisational Structure and Human Resources	This risk focus area evaluates the impact of the ICT solution/ system under consideration on the existing Departmental human resources and or other relevant employees. The focus area further evaluates the extent to which human resources are available and/or are allocated accordingly for the development and/or support of the system/solution going forward.	
26. Client Needs	This risk focus area evaluates whether the proposed/ acquired/developed ICT solution/ system meets the properly defined and documented client needs.	

7. Conclusion

- 7.1 It is imperative to mention that after applying this ICT Risk Management Toolkit, based on the above mentioned Risk Focus Areas, each solution will be rated using an overall total percentage of 100%.
- 7.2 This will be the total rating percentage for the solution. It is expected that the Department should then be able to decide whether to continue or abandon or modify the solution based on the risk rating and recommendations. This Toolkit can be applied in relation to all new and existing ICT solutions.

8. Approval of the ICT Risk Management Toolkit and Date of Effect

This ICT Risk Management Toolkit is Approved ~~/Not Approved~~

Comments:


.....

.....

.....

.....

.....



DR. J. MAC KAY
ACCOUNTING OFFICER

20-08-2023
DATE