# Public Service ICT Risk Management Toolkit

the dpsa
Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

Batho Pele
Putting People First

We Belong
We Care
We Serve

# Table of Contents

# Introduction



- Organizations exist to fulfil the needs of their stakeholders through projects, operations and other activities;
- Citizens are the key government stakeholders;
- Government mostly leverage information and Communication technology (ICT) to fulfil stakeholder needs;
- Despite the differences, activities performed by Departments from carry inherent risk of various types;
- ICT related business risks can be mapped down to poor and or inadequate governance of enterprise IT;
- ICT Risk toolkit seeks to outline and simplify the most common risk scenarios Departments need to cater for before, during and after the acquisition/ development of an ICT solution and or system.
-

# Purpose



- To promote a risk aware behavior by Departments when acquiring, developing and managing ICT systems and or solutions;
- To constantly focus the Departments on the business objectives they seek to achieve when investing and or using ICT and related services;
- To make ICT risk management part of the Departmental management and decision making processes;
- To provide a systematic and logical approach to be followed by the Departments when proactively and reactively managing ICT risks;
- To make Departmental staff aware of risks associated with the usage of ICT and promote responsible risk taking when using this platform;

# Scope and Applicability



- ICT Risk toolkit complements the Public Service Wide Enterprise Risk Management Framework issued by the National Treasury;
- Risk Officers when interacting with OGITO OR GITO engaging a service provider;
- Toolkit assumes that Departments have determined the risk appetite and tolerance levels relevant for their ICT environments;
- National, provincial and local spheres of government when acquiring, developing and or using ICT systems and or solutions as a means to attain their objectives including daily operations ;

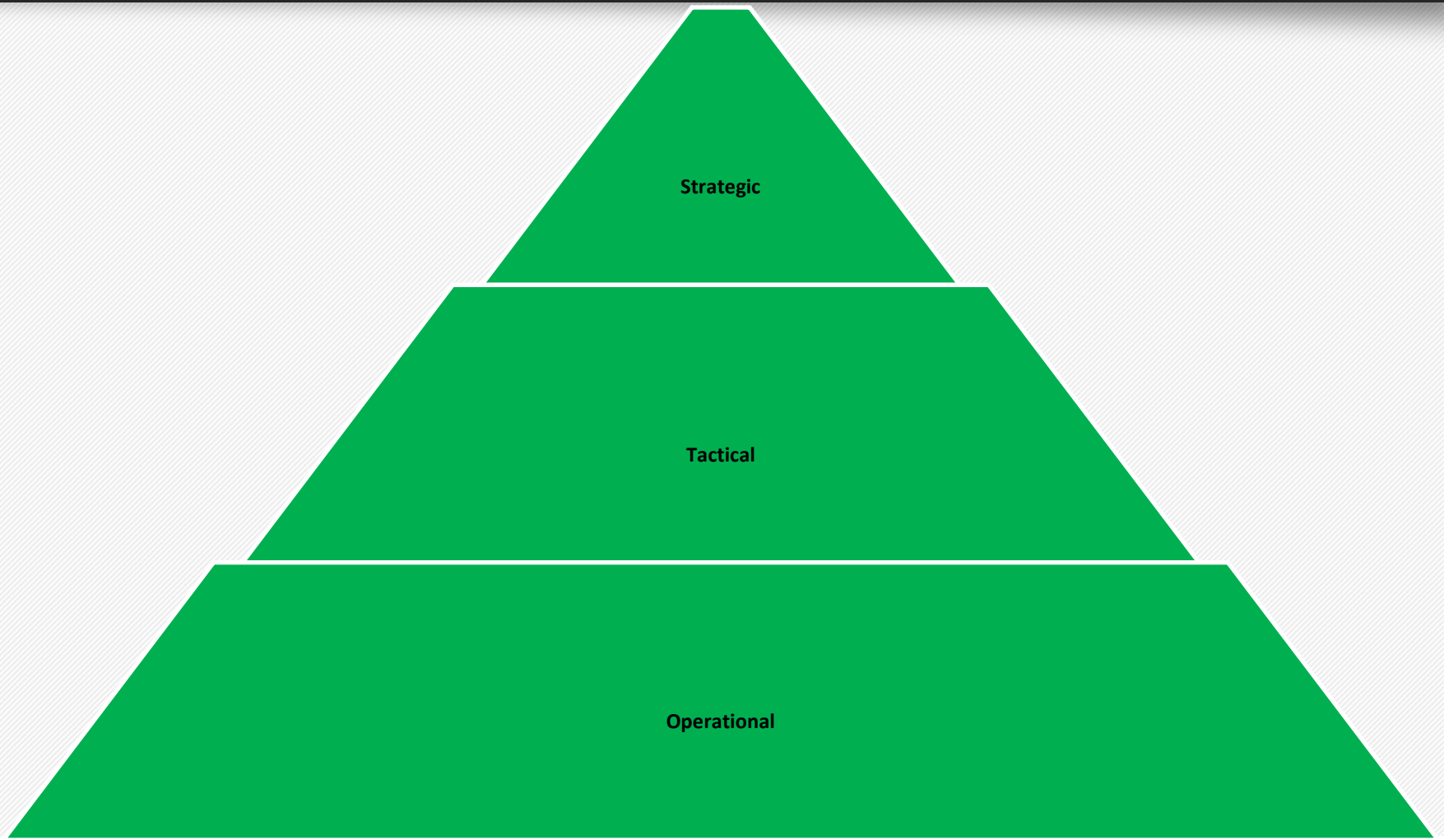
# What is a Risk and Risk Management



- International Standards Organization (ISO 31010: 2009) and the South African National Standards (SANS 31010: 2010), defines Risk as '**the effect of uncertainty on objectives**';
- ICT risks would therefore refer to uncertainty in achieving ICT objectives;
- Risks can only occur within the context of particular objectives, be it they are financial, security, human resources, information technology or related to other functional areas;
- 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 Department faces as it seeks to achieve its ICT and related objectives;

# Risk categories





# Risk categories – *cont.*



- Risks could be categorized as strategic, tactical or operational in nature.
- Risks can also be related to markets (market risks), legislation (compliance risk) environment (environmental risks), politics (political risks), etc.
- Strategic risk = uncertainty in the achievement of the Department's high level and long term (strategic) goals.
- Tactical risk = uncertainty in the achievement of the Department's business goals and objectives mainly due to the approach adopted when trying to achieve them
- Operational risk = uncertainty in the achievement of the Department's business goals and objectives due to inadequacy, ineffectiveness or failure of systems, controls, people, and or processes within the organization

# Risk focus areas



| 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 or 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 including the entire country. | |
| 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 (including business case and decision making processes) and controls have been adhered to or followed during the acquisition and or development of the ICT solution/ system under consideration. | |
| 5. Citizen convenience | This risk focus area evaluates the extent to which the acquired/ developed ICT solution/ system brings about convenience to the citizens. | |

# Risk focus areas – *cont.*



| | | |
|---|---|---|
| 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 implementation 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 areas looks at the contract/ business agreement, service level agreement and other relevant protocols to support the agreement(s) between the Department/ public service and the solution/ system supplier. | |
| 16. Enterprise Architecture | This risk focus area evaluates the extent to which the acquired/ develop 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 solution/ system are understood and have been documented. Optimisation of such processes is also the interest of this risk scenario/ focus area. | |

# Risk focus areas – *cont.*



| | | |
|---|---|---|
| 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 ICTsolution/ system. This focus area further evaluates whether sufficient testing was done on the acquired/ developed ICT solution/ system (i.e. unit, integration, stress testing, end to end, UAT, 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. | |

Dankie / Thank you / Ngiyathokoza

Enkosi / Ngiyabonga / Ke a leboga

Ke a leboha / Ndi a livhuwa

Ndza khensa