Limpopo Province Department of Public Works

Draft GITO Operational Risk Assessment Report

12 December 2006

12 December 2006
This report contains 33 pages

Contents

1 Introduction

We were requested to facilitate a strategic and nine operational risk workshops for the Limpopo Province Department of Public Works (DPW). The first step in this process was to undertake a strategic risk assessment, with a view to best direct Executive Management's efforts towards the highest risks to which DPW is exposed. Accordingly, meetings were held with executive management to identify potential risk areas' threatening the achievement of DPW's strategic objectives prior to the strategic risk workshop which was facilitated by KPMG on 27 November 2006.

Subsequent to the strategic risk workshop an operational risk assessment workshop for GITO was facilitated by KPMG on 7 December 2006 to identify potential risk areas' threatening the achievement of GITO's operational objectives.

The main purpose of this workshop was to involve and assist the General Manager: GITO and Management from the programme in assessing and prioritising the risks that need to be managed in order to achieve the vision and vision of DPW as well as the operational objective of GITO. The workshop was also designed to assist GITO management in the establishment of the risk management process as required by the Public Finance Management Act (PFMA) and best practice corporate governance, as well as provide guidance to the internal audit function in the development of a risk based internal audit strategy and annual internal audit plan for DPW.

The participants included amongst others:

- General Manager: GITO;
- Senior Managers; and
- Managers.

We are pleased to provide you with a summary of the results of the operational risk assessment. The risk assessment information incorporates the participants' perceptions, assumptions and judgments about GITO's operational risks and related controls. **The report does not seek to identify all risks faced by GITO. It focuses only on those operational risks that were highlighted during the workshop by the workshop participants.**

It is important to note that risk management is the responsibility of the General Manager: GITO and Management of the programme. **KPMG's responsibilities are limited to the facilitation of the operational risk assessment (ranking of the identified operational risks).**

A final evaluation regarding the efficiency and effectiveness of the processes and controls in mitigating the identified risks will not be made until the internal audit function perform actual tests during internal audit fieldwork.

1.1 Restriction on distribution of this document

This document has been prepared for the sole and exclusive use of DPW and may not be made available to anyone other than authorised persons within DPW, nor relied upon by any third party without the prior written consent of KPMG.

2 Strategic overview

2.1 Background

The results of the operational risk assessment workshop reflect participants' views only. The facilitators did not attempt to influence the process or results in any way. Their role was merely to gather information in a structured manner and to record the views of the participants.

DPW's vision and mission and GITO's operational objectives are as follows:

2.2 Vision

The **vision** of DPW is:

"A leader in the provision and management of provincial government land and buildings"

2.3 Mission

The **mission** of DPW is:

"Optimal utilisation of resources in the provision and management of provincial land and buildings and the coordination of the implementation of the Expanded Public Work Programme."

2.4 GITO's operational objectives

The **operational objectives** of GITO are as follows:

- *"Improve work efficiency; and*
- *Enhance and strengthen good corporate governance."*

The risk assessment was performed taking the GITO operational objectives into account by consistently asking the question:

"What are the major threats that could prevent GITO from achieving its operational objectives?"

3 KPMG risk assessment approach

An overview of the risk assessment process followed is presented below:

3.1 Methodology

In order for any business to be effective, it must focus its attention and resources on the areas of most significant risk and concern to stakeholders. The risk assessment workshops are fundamental elements of the risk management process.

The principal aims of the operational risk workshop were to:

- Confirm DPW's vision and mission and operational objectives of GITO;
- Confirm the significant and major risks, identified by management threatening the achievement of these objectives;
- Analyse the risks (impact / potential loss, likelihood / probability); and
- Analyse the perceived control effectiveness.

During the workshop, participants were required to provide input based on their actual knowledge and experience of GITO's operations and environment.

3.2 What is risk in a business environment

"Risk is inherent in business processes; it arises from actions taken in pursuit of objectives and changes in the external environment. Change in the ways companies do business, in technological developments, in the regulatory framework and the size of the business in terms of the strain such change places on its control mechanisms are all major sources of risk."

-Sir Roger Hurn (Chairman of Marconi plc)

3.2.1 Risk definition for the purpose of the workshop

For purposes of the workshop and implementing an effective risk management system at GITO, a risk / threat was defined as follows:

"Uncertain future events, which could influence the achievement of the entity's objectives."
- King II

For each risk / threat identified the following was assessed:

3.2.1.1 The impact

This is the **potential magnitude of the impact** on GITO's operations **should the risk / threat actually occur**. No account of existing controls is taken into consideration in assessing the impact of risks. The impact was categorised into 5 different levels, namely:

Catastrophic	Critical	Serious	Significant	Minor

For a detailed explanation of the different categories please refer to **Appendix A**.

3.2.1.2 The probability of occurrence

This is the likelihood that the identified risk / threat will occur within a specified period of time (between 1 and 3 years) on the basis that **management have no specific / focused controls in place to address the risk / threat.** The probability of occurrence was categorised into 5 different levels, namely:

Almost certain	Likely	Possible	Unlikely	Rare

For a detailed explanation of the different categories please refer to **Appendix A**.

3.2.2 Inherent risk

Inherent risk is the *product of the impact of a risk and the probability of that risk occurring before the implementation of any direct controls.* The score for inherent risk assists management and internal audit alike to establish relativity between all the risks / threats identified. Please note that at this stage no account is taken of existing controls implemented by management.

This indicator may be used to assign / measure the level of management effort / resources required to control the relevant risks and to determine the level of internal audit focus required.

3.2.3 Controls

Controls are the processes / functions / programmes that Management and the General Manager: GITO have put in place, and rely upon, to manage the major and significant risks. At this operational risk assessment workshop we have limited ourselves to the ranking of the perceived effectiveness of these processes.

3.2.4 Perceived control effectiveness

The participants **assessed the control effectiveness based on their understanding of the control environment currently in place at DPW**. This is a measure of how well management perceives the control processes to be working and effectively managing the risks. Processes / controls were categorised into 5 different levels of effectiveness, namely:

Very good	Good	Satisfactory	Weak	Unsatisfactory

For a detailed explanation of the different categories please refer to **Appendix A**.

3.2.5 Residual risk

This is the score of risk that GITO is exposed to taking into account the potential impact of the risk, the probability of the risk occurring and the related control processes which are in place to manage that risk. *Residual risk / exposure is therefore the product of the inherent risk and the control effectiveness factor.*

This information will assist decision makers in assessing the acceptability of the residual risk / exposure and in deciding whether further management action is required to effectively control the risk.

3.2.6 Management actions

Based on the relative score of the residual risk / exposure, **management will need to decide whether or not they are willing to accept the identified level of residual risk / exposure.**

If the residual risk is considered to be too high, then an action plan will then need to be developed outlining the identified action/s to reduce the risk to a level that is more acceptable to management and other stakeholders.

Management actions may include the re-examination of the control design and / or the business / quality objective identified earlier in the risk management process.

The action plans must clearly identify:

- The required action;
- The person responsible for implementing the action; and
- The expected date of implementation.

4 Results

The workshop participants agreed and confirmed the vision and mission of DPW as well as the operational objectives of GITO. The risks identified by the workshop participants of GITO were rated and the control effectiveness of the managing processes and / or persons currently responsible to mitigate or manage each of these risks was also assessed in terms of perceived control effectiveness.

Participation and discussion during the workshop was open and constructive. We were particularly impressed with the level of attendance of the participants.

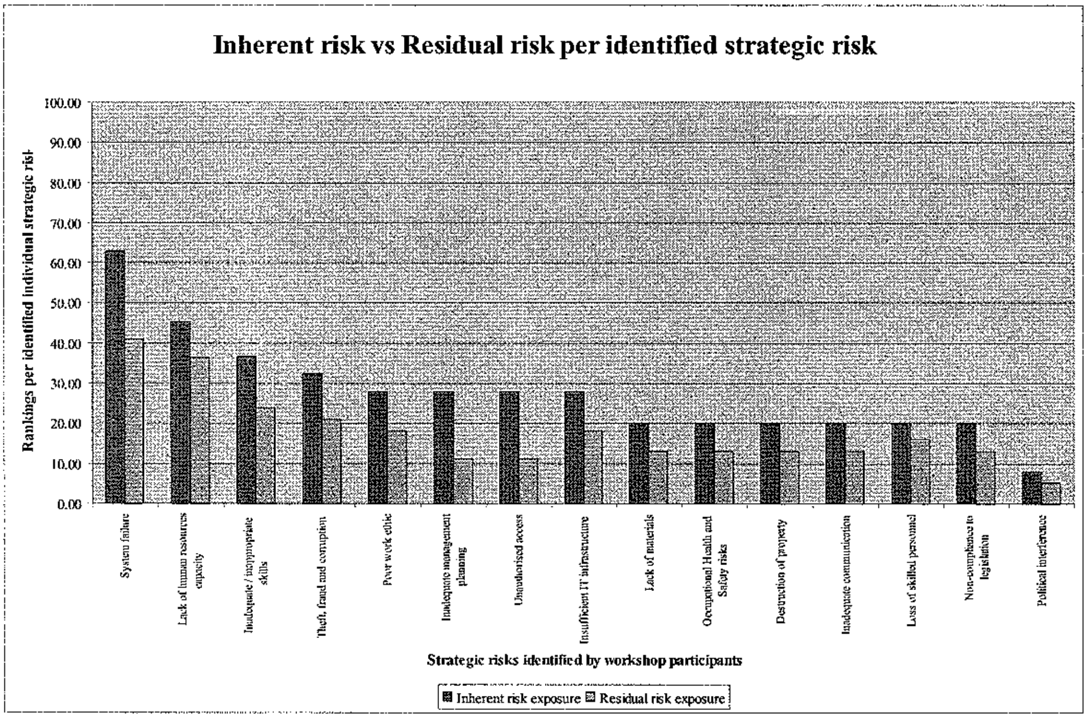
The results of the risk assessment workshop, from highest to lowest inherent risk, have been depicted graphically in **Paragraph 4.1**.

The major / significant risks currently faced by GITO, as identified by the participants during the strategic risk workshop, are presented in **Paragraph 4.2** from highest to lowest inherent risk.

4.1 Graphical illustrations

4.1.1 General

The identified operational risks are depicted graphically below.



4.1.2 Risk graph

The relative size of operational risks threatening the achievements of DPW's vision and mission and operational objectives of GITO as well as the perceived control effectiveness for each of the risks, as identified by the workshop participants, are depicted graphically above from the highest to the lowest inherent risk.

The inherent nature of the risk is the assessment of the risk without specific, focused controls in place. The residual nature of the risk is the assessment of the risk taking into account the existing controls and their perceived effectiveness.

The larger the difference between the inherent and residual risk factors the more effective the controls in place are perceived to be.

The smaller the difference between the inherent and residual risk factors, the more management actions and improved control effectiveness is needed to ensure that the risk is properly managed.

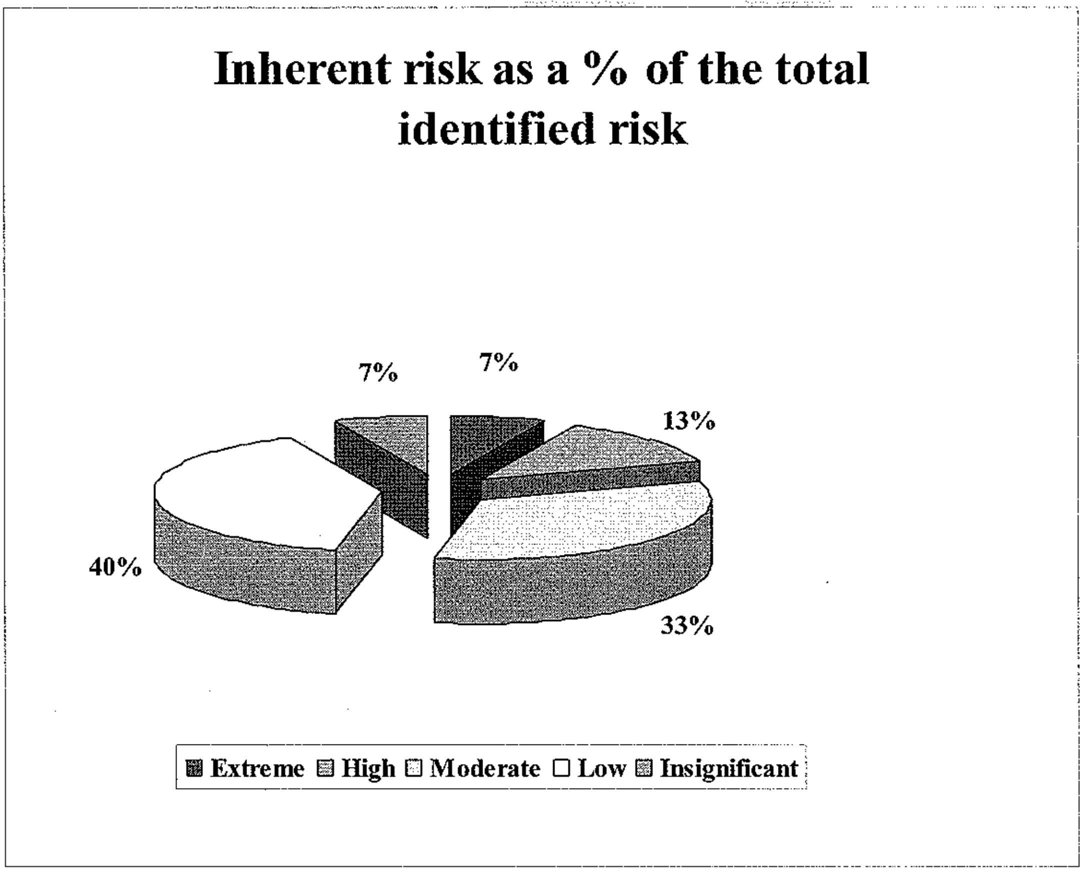
Management should take cognisance that the higher the inherent risk factor, the greater the need for control effectiveness and therefore the more management attention the item should attract in order to:

- Maintain the quality of control where control effectiveness is considered adequate; and

- Improve quality of control further where residual risk is considered to be too high.

4.1.3 Inherent risk

Of the 15 operational risks identified by Management of GITO 1 (7%) was assessed as extreme by the participants attending the risk workshop.



Risks rated with extreme inherent risk ratings are as follows:

- System failure.

Risks rated with high inherent risk ratings are as follows:

- Lack of human resources capacity;
- Inadequate / inappropriate skills.

Risks rated with moderate inherent risk ratings are as follows:

- Theft, fraud and corruption;
- Poor work ethic;
- Inadequate management planning;
- Unauthorised access; and
- Insufficient IT infrastructure.

Risks rated with low inherent risk ratings are as follows:

- Lack of materials;
- Occupational health and safety risks;
- Destruction of property;
- Inadequate communication;
- Loss of skilled personnel; and
- Non compliance to legislation.

Risks rated with insignificant inherent risk ratings are as follows:

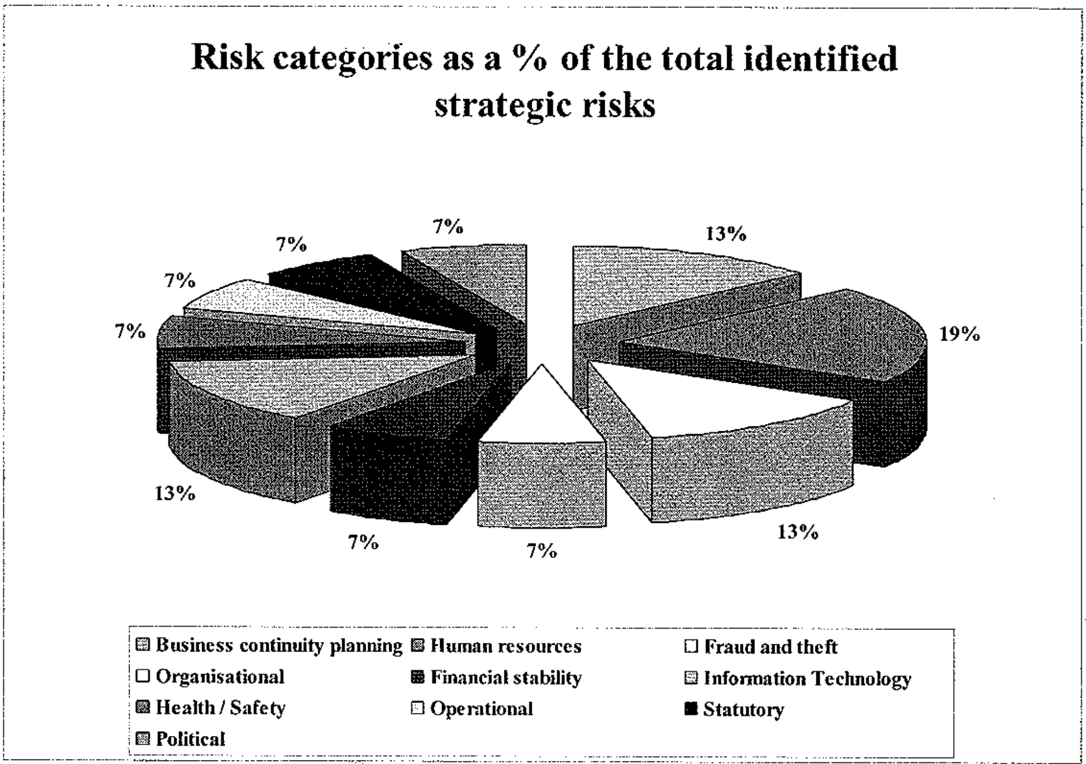
- Political interference.

The above analysis clearly illustrates the importance of focusing and actively managing the highest risk areas first and then gradually working down the list.

The higher the inherent risk value, the greater the need for good quality controls and control effectiveness and the more Management, General Manager: GITO and Internal Audit attention the item should attract.

4.1.4 Identified risk categories

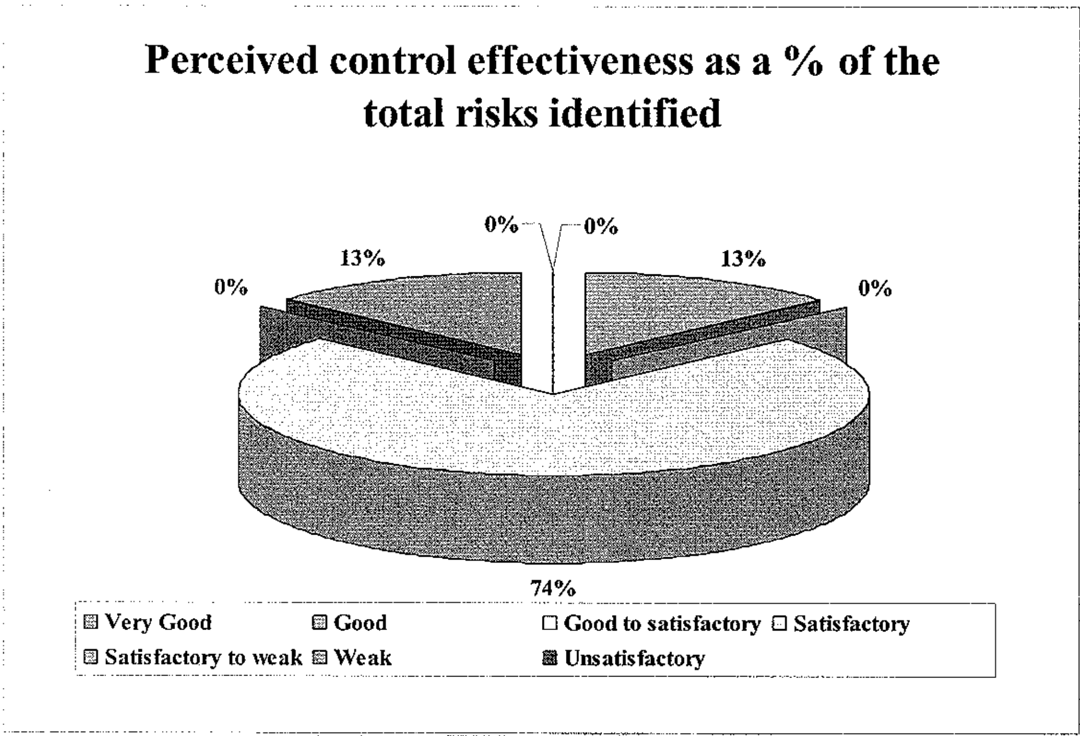
The 15 operational risks identified by management were categorised into 10 identified risks categories. This clearly indicates that risk from both an internal and external environment were identified. It also clearly indicates that risk from both core and support processes were identified.



Once again Management should assess whether the assessments and this analysis is correct and take appropriate corrective action.

4.1.5 Perceived control effectiveness

As indicated above, 15 operational risks were identified by management. Of the 15 operational risks identified by management 2 (13%) were evaluated as weak by the participants attending the workshop.

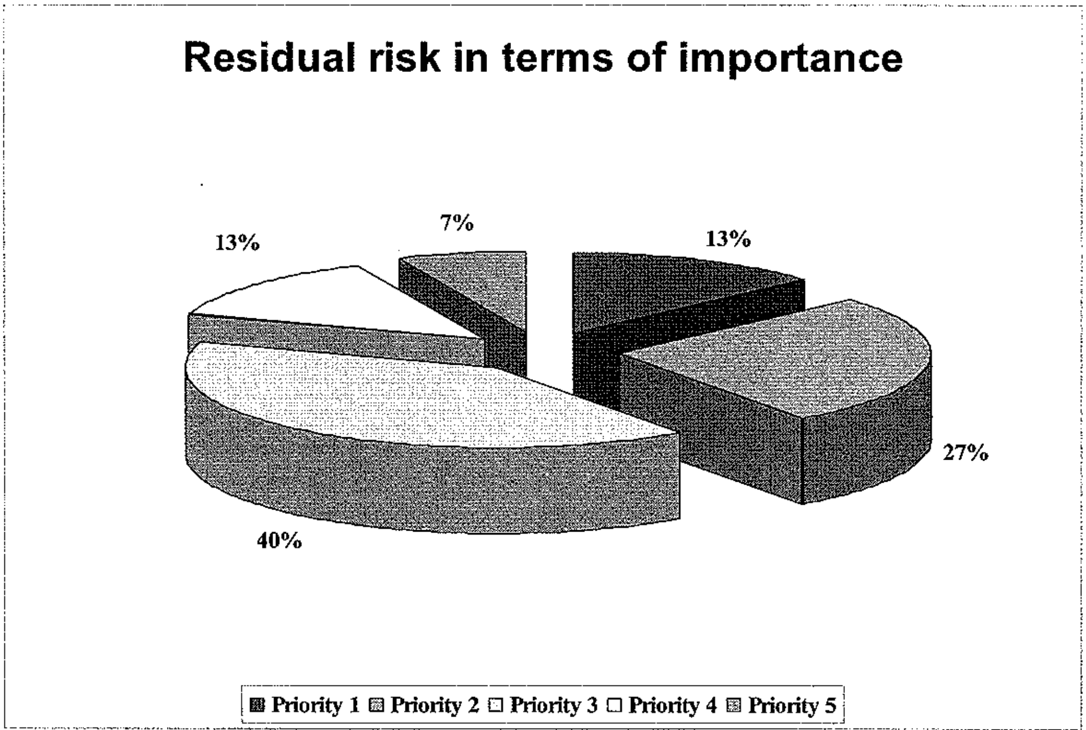


87% of controls managing the operational risks are perceived to be either satisfactory or good. Management should assess whether the assessments and this analysis is correct and take appropriate corrective action.

4.1.6 Residual risk

The residual graph represents the highest assessed risks faced by GITO after taking into account the existing controls and their perceived control effectiveness. The higher the residual risk, the greater GITO's exposure to loss or loss of opportunities. These areas should be a guide as to the priority for management effort and the allocation of resources to improve the design / quality of control and control effectiveness.

The graph below indicates the residual risk in terms of importance / priorities.



The KPMG Risk Methodology classifies and defines residual risk as the following priorities:

Priority 1: The risk is intolerable and requires action to further mitigate the exposure;

Priority 2: The risk is intolerable and requires management intervention to further mitigate the exposure;

Priority 3: This risk exposure exceeds the current risk appetite and should be monitored to ensure prompt intervention if so required;

Priority 4: The risk exposure is tolerable; and

Priority 5: Risk may be over controlled.

As indicated in the graph above, 80% of the identified and assessed risks in terms of residual risk are assessed as requiring management intervention.

*Strategic risks rated as **Priority 1** risks are as follows:*

- System failure; and
- Lack of human resources capacity.

*Strategic risks rated as **Priority 2** risks are as follows:*

- Inadequate / inappropriate skills;
- Theft, fraud and corruption;
- Poor work ethic; and
- Insufficient IT infrastructure.

*Strategic risks rated as **Priority 3** risks are as follows:*

- Lack of materials;
- Occupational health and safety risks;
- Destruction of property;
- Inadequate communication;
- Loss of skilled personnel; and
- Non compliance to legislation.

*Strategic risks rated as **Priority 4** risks are as follows:*

- Inadequate management of planning; and
- Unauthorised access.

*Strategic risks rated as **Priority 5** risks are as follows:*

- Political interference.

4.2 Summary of operational risks confirmed during the workshop

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
1	**System failure** - Power failure - Network unavailability	Loss of productivity Increased cost of service delivery Financial loss Poor decision making process Inaccurate corporate reporting	1, 2	Business continuity planning	Key assets	Senior Manager: ICT	70.00	0.90	63.00	Back-up power supply Approved and implemented disaster recovery plan Approved and implemented infrastructure plan Signed Service Level Agreement (SLA) with State Information Technology Agency (SITA) for outsourced transversal systems and WAN	0.65	Develop infrastructure blueprints **Deadline date: 30 June 2007** **Responsible Official: Senior Manager: ICT** Investigate possibility of hosting and hosting management **Deadline date: 28 February 2007** **Responsible Official: Senior Manager: ICT** Re-visit relevant policies and procedures **Deadline date: 30 June 2007** **Responsible Official: Senior Management: ITC**	40.95
2	**Lack of human resources capacity**	Increase in cost Decrease in quality Lower productivity	1, 2	Human Resources	Key assets	General Manager	70.00	0.65	**45.50**	Approved and implemented organogram for GITO	0.80	Motivate need for funding of posts to MEC **Deadline date: 28 February 2007**	36.40

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
		Inability to meet targets and deadlines								Approved annual plan for GITO linking budgets to outcomes Monthly reporting on vacancies at management meeting		**Responsible Official: General Manager** Investigate possibility of implementing learnerships **Deadline date: 28 February 2007** **Responsible Official: General Manager**	
3	**Inadequate / inappropriate skills** - Insufficiently skilled staff - Mismatched skills	Inability to meet targets Cost inefficiencies Poor quality of service delivery Institutional memory loss Lack of continuity	1, 2	Human Resources	Key assets	Senior Managers	70.00	0.53	36.75	Approved and implemented Performance Management System Skills audit (Sep 2006) Approved Workplace Skills Plan Individual Development Plan Informal on the job training Attendance of formal training Approved organisational structure Implemented recruitment processes Approved job descriptions	0.65	Develop multi skilling strategy **Deadline date: 30 June 2007** **Responsible Official: General Manager** Investigate possibility of implementing learnerships **Deadline date: 28 February 2007** **Responsible Official: General Manager** Motivate individual training **Deadline date: 28 February 2007** **Responsible Official: All Senior**	23.89

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
										Budgetary process linked to organisational structure Implemented HR policies and procedures		**Managers**	
4	**Theft, fraud and corruption** - Nepotism	Financial loss Harm to reputation Inability to meet targets	1, 2	Fraud and theft	Key assets Alliances	General Manager	50.00	0.65	**32.50**	Approved and implemented policies and procedures Segregation of duties IT assets management Physical and logical security Existing contracts with all suppliers Use of registers for movement of assets Approved and implemented disciplinary procedures for transgressors Use of National anti-fraud and corruption hot line	0.65	Re-visit policies and procedures **Deadline date: 30 June 2007** **Responsible Official: All Senior Managers** Implement Fraud Awareness campaigns **Deadline date: 31 August 2007** **Responsible Official: Senior Manager: Communication** Establish ICT steering committee **Deadline date: 31 January 2007** **Responsible Official: General Manager**	**21.13**

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
5	**Poor work ethic** - Absenteeism - Poor time management	Harm to reputation Lack of accountability Inability to meet targets and deadlines Cost inefficiencies Poor quality of service delivery	1, 2	Organisational	Strategic Management Process	Senior Managers	70.00	0.40	**28.00**	Approved and implemented leave policies and procedures Use of attendance registers Implemented disciplinary procedures for transgressors Approved and implemented Code of Conduct Implemented Employee Assistance Programme Supervision Implemented Performance Management System	0.65	Implementation of work ethic awareness campaigns **Deadline date: 30 April 2007** **Responsible Official: Senior Manager: Communications** Employee satisfaction survey **Deadline date: 28 February 2007** **Responsible Official: Senior Manager: Communications** Implementation of service excellence awards **Deadline date: 31 January 2007** **Responsible Official: Deputy Manager: Information Management**	**18.20**
6	**Inadequate management planning** - Insufficient budget	Harm to reputation Inability to meet targets Poor quality of service delivery	1	Financial stability	Key assets	General Manager	70.00	0.40	**28.00**	Approved and implemented Medium Term Expenditure Framework (MTEF)	0.40	Investigate possibility of including districts in budget planning **Deadline date: 31 January 2007**	**11.20**

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
										Approved and implemented 5 Year Strategic Plan Approved and implemented Operational Plans Monthly reporting on actual versus budget Monthly directorate meetings to discuss progress on projects etc		**Responsible Official: All Senior Managers** Implementation of projected cash flows **Deadline date: 31 January 2007** **Responsible Official: Deputy Manager: Facilities**	
7	**Unauthorised access** - Records - Information	Harm to reputation Negative public perception Fraud and corruption Financial loss	2	Fraud and theft	Key assets	Senior Manager: IRM Senior Manager: ICT	70.00	0.40	**28.00**	Implementation of policies, procedures and legislation Implemented logical access controls Implemented physical access controls Use of registers to record document movement Use of incidents registers	0.40	Investigate security risk for repository **Deadline date: 31 March 2007** **Responsible Official: Senior Manager: ICT and Senior Manager: IRM** Awareness of Promotion of Access to Information Act **Deadline date: 31 March 2007** **Responsible Official: Senior Manager: IRM**	**11.20**

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
8	**Insufficient IT infrastructure** - LAN connectivity - Storage space	Inability to meet targets and deadlines Poor quality of service delivery	1	Information technology	Key assets	Senior Manager: ICT	70.00	0.40	**28.00**	Approved and implemented Medium Term Expenditure Framework (MTEF) Approved and implemented infrastructure plan	0.65	Investigation of connectivity alternatives **Deadline date: 28 February 2007** **Responsible Official: Senior Manager: IRM** Development of storage plans **Deadline date: 31 March 2007** **Responsible Official: Senior Manager: IRM**	**18.20**
9	**Lack of materials** - Hardware - Resources	Inability to meet targets and deadlines Poor quality of service delivery	1	Information technology	Key assets	Senior Managers	50.00	0.40	**20.00**	Performance of IT Needs Analysis Approved and implemented Medium Term Expenditure Framework (MTEF) Approved and implemented procurement policies	0.65	Performance of IRM needs analysis **Deadline date: 28 February 2007** **Responsible Official: Senior Manager: IRM** Performance of a communication needs analysis **Deadline date: 28 February 2007** **Responsible Official: Senior Manager: Communication**	**13.00**

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
10	**Occupational Health and Safety risks** - Fire - Water damage - Injuries	Loss of life Injuries to employees Decrease in productivity Increase in operating costs Negative corporate image Loss of information	1, 2	Health / Safety	Key assets	Deputy Manager: Information Management	50.00	0.40	**20.00**	Approved and implemented occupational health and safety policies and procedures Identified and appointed OHS representatives Reporting of injuries on duty Implemented OHS awareness campaigns Approved and implemented disaster recovery plan	0.65	Implementation of OSHA awareness training **Deadline date: 30 April 2007 Responsible Official: Deputy Manager: Information Management** Implementation of internal audit recommendations **Deadline date: 31 March 2007 Responsible Official: Senior Manager: ICT** Develop and implement business continuity plan for GITO **Deadline date: 30 September 2007 Responsible Official: Senior Manager: IRM**	**13.00**
11	Destruction of property - Damage to records	Inability to meet targets and deadlines Financial loss Poor quality of service delivery Institutional memory loss	1, 2	Business continuity planning	Key assets	Senior Manager: IRM Senior Manager: ICT	50.00	0.40	**20.00**	Approved and implemented disaster recovery plan Implemented physical security	0.65	Develop Business Continuity Plan **Deadline date: 30 September 2007 Responsible Official: Senior Manager: IRM**	**13.00**

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
										Implementation of policies, procedures and legislation (National and Provincial archives Act) Use of fire fighting equipment		Investigate possibility of digitising records management **Deadline date: 31 March 2007** **Responsible Official: Senior Management: IRM & Senior Manager: ICT**	
12	**Inadequate communication** - Mis communication - Mis understanding	Silo mentality Inability to share information Harm to reputation Cost inefficiencies Inability to meet targets	1, 2	Operational	Key assets	Senior Manager: Communication	50.00	0.40	**20.00**	Formalised monthly programme meetings Use of intranet site Approved and implemented communication strategy and policy Monthly internal and quarterly external news letters Approved marketing and advertising activities Implemented communication standards MEC radio interviews, etc.	0.65	Improve internet and intranet websites **Deadline date: 30 June 2007** **Responsible Official: Senior Manager: IRM** Implement internal audit recommendations (translation) **Deadline date: 30 April 2007** **Responsible Official: Senior Manager: Communication** Develop Communication Plan **Deadline date: 28 February 2007** **Responsible Official: Senior**	**13.00**

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
										Use of service excellence awards		**Manager: Communications** Investigate possibility of utilising digital communication boards **Deadline date: 28 February 2007** **Responsible Official: Senior Manager: Communication**	
13	**Loss of skilled personnel** - Inability to retain skilled personnel	Inability to meet targets Cost inefficiencies Poor quality of service delivery Institutional memory loss Lack of continuity	1, 2	Human Resources	Key assets	Senior Managers	50.00	0.40	**20.00**	Implemented retention plan (including counter offers) Performance Management System Job evaluations Implemented annual skills work place plan Use of exit interviews	0.80	Develop and implement multi skilling strategy **Deadline date: 30 June 2007** **Responsible Official: General Manager** Motivate individual training **Deadline date: 28 February 2007** **Responsible Official: All Senior Managers** Motivate reasons for counter offers **Deadline date: Ongoing**	**16.00**

Strategic risk number	Risk description	Consequence of risk	Link to strategic focus area	Risk categories	Link to dependency profile	Risk owner	Impact	Likelihood	Inherent risk exposure	Current controls	Perceived control effectiveness	Additional actions	Residual risk exposure
												Responsible official: All Senior Managers	
14	**Non-compliance to legislation**	Possible prosecution Financial loss Negative publicity and harm to reputation	2	Statutory	Key assets External forces and agents	General Manager	50.00	0.40	**20.00**	Compliance awareness campaigns Monthly IRM meetings (compliance to legislation discussed at these meetings) Implemented systems compliance checklist Performance of system audits Performance of assets audits Subscription to Sabinet	0.65	Formalise compliance calendars **Deadline date: 31 March 2007** **Responsible Official: Senior Manager: IRM**	**13.00**
15	**Political interference**	Inability to meet targets Inability to meet deadlines	1, 2	Political	External forces and agents	General Manager	40.00	0.20	8.00	Approved and implemented 5 Year Strategic Plan Implemented policies and procedures relating to political interference	0.65	None identified	5.20

5 The way forward

Having completed the GITO risk assessment (a key step in the overall risk management process), management now needs to focus on ensuring it understands the risk universe within which it operates. Achieving the operational intent within the risk universe involves identifying what has to be managed and ensuring that such management and control actually takes place timeously and effectively.

The operational level risk assessment workshop has provided a basis for commencing the implementation of a formal risk management framework at GITO.

The next challenge is to develop and implement a structured plan for implementing effective and ongoing risk management at GITO.

This should include the following key phases and steps, amongst others:

5.1.1.1 Project planning

Develop a detailed project plan to implement Enterprise-wide Risk Management at GITO, meeting the key requirements of:

- The Public Finance Management Act;
- the King Report on Corporate Governance (King 2); and
- the Standards of the Institute of Risk Managers of South Africa.

5.1.1.2 Risk awareness and strategy

- Develop and rollout an ongoing risk management awareness and training programme for all levels of management – to build upon the current level of understanding and knowledge.
- Establish ownership and accountability for risk management within GITO - Incorporate risk responsibilities in key management mandates, charters, performance contracts, job descriptions, etc.
- Include risk management as a key agenda item on key meetings, e.g. Executive Management.
- Gradually formalise and approve a risk strategy that is aligned with and supports the achievement of GITO's operational direction.

5.1.1.3 Risk management structures and culture

- Ensure an independent committee is formally charged with overseeing the risk management process – this may form part of the Executive Committee mandate or may be allocated to a separate body that reports back at Executive Committee meetings.
- Appoint / identify a dedicated "Chief Risk Officer" responsible for coordinating and analysing GITO's risk management and assurance efforts on an ongoing basis, and reporting to key stakeholders.
- Establish a team of "Risk Champions" who will work closely with the "Chief Risk Officer" and will drive the risk management initiatives within their respective directorates.

5.1.1.4 Integrated risk assessments and risk management activities

- Maintain the Operational Risk Register current and up to date – including a formal risk identification and assessment process conducted at least annually.
- Incorporate the identified operational risks into both the operational plan for 2007 / 2009 and the annual plans.
- Allocate responsibility for each individual major risk to a senior (and accountable) member of management (risk owner) – including the implementation of management action plans to improve levels of control where required.
- Regular management / monitoring of the identified exposures through:
  - Further development of specific action plans to address individual exposures;
  - Allocation of individual officials responsible for action plans;
  - Setting of due dates / implementation of time frames;
  - Development of key performance indicators by which the success of the improved controls can be measured; and
  - Facilitation of sub-process level risk workshops.

  Sub-process level risk workshops should be conducted to reach consensus regarding:

  - Related sub-process level objectives and risks;
  - The alignment of the above with operational focus areas as well as the risks identified in this report;
  - Controls which management relies upon to manage those risks;
  - Perceived and desired effectiveness of those controls; and
  - Areas considered to be lacking in control, which would require further management action.

- Integrate the active monitoring of identified risks and related controls (including the allocation of individual "risk owners") into the ongoing activities of the Directorates, Management, General Manager: GITO and the Risk Committee;
- Ensure there is regular report-back by the "risk owners" on the status of the risks and related internal controls – This should be performed as part of the normal management activities, e.g. monitoring performance against "risk based" business plans and budgets.

A GITO specific risk management framework developed through this process will not only ensure that best practice corporate governance requirements are adhered to but will also improve the effectiveness of management in discharging their own management and governance responsibilities.

6 Acknowledgements

We would like to thank the General Manager: GITO and all workshop participants of GITO for their cooperation and participation in the workshop.

Appendix A – Dependency Profile

Draft GITO Dependency Profile

External Forces and Agents

Legislation
Socio Economic Environment
Political
Geographical spread
Media
Environmental
Macro Economy
Technology

Strategic Objectives

Improve work efficiency

Enhance and strengthen good corporate governance

Strategic Management Process

Strategic issues

Key assets

Cash and Bank
Land
Buildings
Information Technology assets
Vehicle fleet
Equipment and Furniture
Intellectual capital and skills
Reputation

Markets

Other divisions within DPW

Citizens

Business

All tiers of Government

Interest Groups

Segmentation

Information Communication Technology

Information and records management

Communication Services

Alliances

Other business units within DPW

National Ministry

Other Limpopo Provincial Department

Public / Private Partnerships

Municipalities

Preferred service providers

Contractors

Non profit organisations

Trade unions

Professional institutions

Competitors

Private Sector
Contractors

Appendix B - Assessment tables

Below are the tables used to size the risks according to the potential impact of the risk, the likelihood that the risk will occur, as well as the effectiveness of existing controls. The following three tables provide the legends for the respective decisions required during the workshop.

Qualitative assessment of impact

The table below was used to assist management in quantifying the impact of a specific risk occurring.

Impact	Continuity of Supply	Safety & Environmental	Technical Complexity	Financial
Catastrophic **100**	Risk event will result in widespread and lengthy reduction in continuity of supply to customers of greater than 48 hours	Major environmental damage Serious injury (permanent disability) or death of personnel or members of the public Major negative media coverage	Use of unproven technology for critical system / project components High level of technical interdependencies between system / project components	Significant cost overruns of >20% over budget Affect on revenue / asset base of >10%
Critical **70**	Reduction in supply or disruption for a period ranging between 24 & 48 hours over a significant area	Significant injury of personnel or public Significant environmental damage Significant negative media coverage	Use of new technology not previously utilised by the entity for critical systems / project components	Major cost overruns of between 10 % & 20 % over budget Affect on revenue / asset base of between 5% & 10%
Serious **50**	Reduction in supply or disruption for a period between 8 & 24 hours over a regional area	Lower level environmental, safety or health impacts Negative media coverage	Use of unproven or emerging technology for critical systems / project components	Moderate impact on revenue and assets base
Significant **30**	Brief local inconvenience (work around possible) Loss of an asset with minor impact on operations	Little environmental, safety or health impacts Limited negative media coverage	Use of unproven or emerging technology for systems / project components	Minor impact on revenue and assets base
Minor **10**	No impact on business or core systems	No environmental, safety or health impacts and/or negative media coverage	Use of unproven or emerging technology for non-critical systems / project components	Insignificant financial loss

Qualitative assessment of probability of likelihood

The table below was used to assist management in quantifying the likelihood of a specific risk occurring.

Likelihood Factor	Qualification Criteria	Rating
Almost Certain	The risk is almost certain to occur in the current circumstances	**0.90**
Likely	More than an even chance of occurring	**0.65**
Possible	Could occur quite often	**0.40**
Unlikely	Small likelihood but could happen	**0.20**
Rare	Not expected to happen - Event would be a surprise	**0.10**

Qualitative assessment of perceived control effectiveness

The table below was used to assist management in quantifying the perceived effectiveness of controls to mitigate or reduce the impact of specific risks.

Effectiveness Factor	Qualification Criteria	Rating
Very Good	Risk exposure is effectively controlled and managed	**0.20**
Good	Majority of risk exposure is effectively controlled and managed	**0.40**
Satisfactory	There is room for some improvement	**0.65**
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	**0.80**
Unsatisfactory	Control measures are ineffective	**0.90**

Inherent Risk

The table below was used to categorise the inherent risk exposure of the identified risks into the 5 different categories.

Inherent Risk	Rating
Extreme	≥ 50
High	≥ 35 < 50
Moderate	≥ 25 < 35
Low	≥ 15 < 25
Insignificant	< 15

Residual Risk

The table below was used to categorise the residual risk exposure into the 5 different categories.

Residual Risk	Rating
Priority 1	≥ 25
Priority 2	≥ 17.5 < 25
Priority 3	≥ 12.5 < 17.5
Priority 4	≥ 7.5 < 12.5
Priority 5	< 7.5