dpwr

Department:
Public Works and Roads
North West Provincial Government
Republic of South Africa

RISK MANAGEMENT STRATEGY 2018/19

TITLE : RISK MANAGEMENT STRATEGY

DEPARTMENT : PUBLIC WORKS AND ROADS

CONTENTS **PAGE NO**

THE RISK MANAGEMENT STRATEGY

1. BACKGROUND

1.1 Managing risks is fundamental to the business of an organisation. The PFMA through section 38(1) (a) (i) requires the Accounting Officer to ensure that the Department has and maintains effective, efficient and transparent systems of financial and risk management and internal control.

1.2 The King IV Report prescribes that the governing body should govern risks in a way that supports the organisation in setting and achieving its strategic objectives.

1.3 The DPWR will adopt an enterprise wide risk management (ERM) strategy which means that every key risk in each part of the Department will be included in a structured and systematic process of risk management. It is expected that the risk management processes will become embedded into the Department's systems and processes, ensuring that our responses to risk remain current and dynamic. All risk management efforts will be focused on supporting the Department's objectives. Equally, they must ensure compliance with relevant legislation, and fulfil the expectations of employees, communities and other stakeholders in terms of corporate governance.

DEFINITION

2.1 **Risk** is the possibility of an uncertain event (threat or opportunity) occurring that will have an impact on the achievement of objectives. It is measured in terms of **impact** (extend of damage that it could cost) and the **likelihood** (the probability) of it occurring.

2.2 **RISK MANAGEMENT**- a continuous, proactive and systematic process, affected by the senior management and all personnel, applied in strategic planning and across the department designed to define, identify, assess risk for impact and materiality and then device mechanisms to reduce risk to tolerance levels as to provide reasonable assurance on the achievement of the organisations objectives.

2.3 **Enterprise Wide Risk Management (ERM) -** Strategic process to enable DPWR to identify measure and manage entire range of business risk and opportunities it is facing.

2.4 **Risk register**- action plan listing residual risk, risk owner, action plans and deadlines.

2.5 **Residual risk**- difference between inherent risk ratings and control rating. Risk value left after control measures have been designed to reduce the inherent/absolute risk.

2.6 **Inherent risk** – risk the department has inherited for conducting business.

2.7 **Risk appetite** – a set maximum level of residual risk the department is willing to take.

2.8 **Risk acceptable level** – It is equal to or below the risk appetite. The department is not going to allocate resources to deal with this risk.

2.9 **Corporate Governance –** Corporate governance involves mechanisms by which an organisation is directed and controlled. It is a corporate tool through which corporate management is held accountable for corporate conduct and performance. It is a strategic response to risk management.

2.10 **Internal Controls -** Mechanisms put into place to mitigate unacceptable levels of risk. Internal controls are a management's responsibility.

2.11 Fraud Prevention strategy/Plan- Strategic process to enable DPWR to identify measure and manage the fraud risk within its systems. Fraud is further defined as an intentional distortion of financial information or other records by a person internal/external to the Department, carried out to conceal misappropriation of assets or otherwise for personal gain.

3. THE RISK MANAGEMENT METHODOLOGY

3.1 Adopted process outlined below:

3.1.1 Objective→ risk → control. It will start with reviewing the strategic objectives to establish goals for which achievement may be impaired by uncertain events (threats and opportunities) **= strategic planning & risk identification.**

3.1.2 Events with negative impact (risk) to be listed, classified and analysed **= risk assessment**.

3.1.3 Controls to be listed, classified and analysed = **control self assessment**

The COSO Enterprise Risk Management- Integrated Framework and Public Sector Risk Management Framework form the basis of the Departmental Strategy.

N.B. The Departmental objectives will be viewed in the context of four categories:

- Strategic
- Operations
- Reporting
- Compliance

3.2 The Department will:

3.2.1 Appoint a risk management committee to help it realise its risk management obligation.

3.2.2 Appoint a Chief Risk Officer to coordinate the risk management process.

3.2.3 Draft a Risk Management policy **(RISK MANAGEMENT PHILOSOPHY)** to set a tone for the risk management activities as part of its strategy.

3.2.4 Set the risk appetite/ tolerance or acceptance levels to facilitate decision making concerned with how to address the risk.

3.2.5 Produce a risk register through which the identified risks will be monitored.

4. RISK IDENTIFICATION

4.1 This is best practice, integral part of risk management and management's responsibility. It cannot be relegated to a one time static process. The department is operating within a dynamic environment with constant political changes. It is therefore prudent for management to consider risk identification as ongoing and continuous

- Strategic Risks: These are risks emanating from the strategic choices made by the department and they will also appear on the departmental strategic plan.
- Operational Risks: These are the risks that will be identified by employees and they should be repeated when changes occur or at least once a year to identify new and emerging risks.
- Fraud Risks: These risks should also be identified by internal and external stakeholders

4.2 **Ask following questions**: What are the threats relative to the achievement of a specific objective?

4.2.1 Two main approaches are (1).Exposures and (2).The environment.

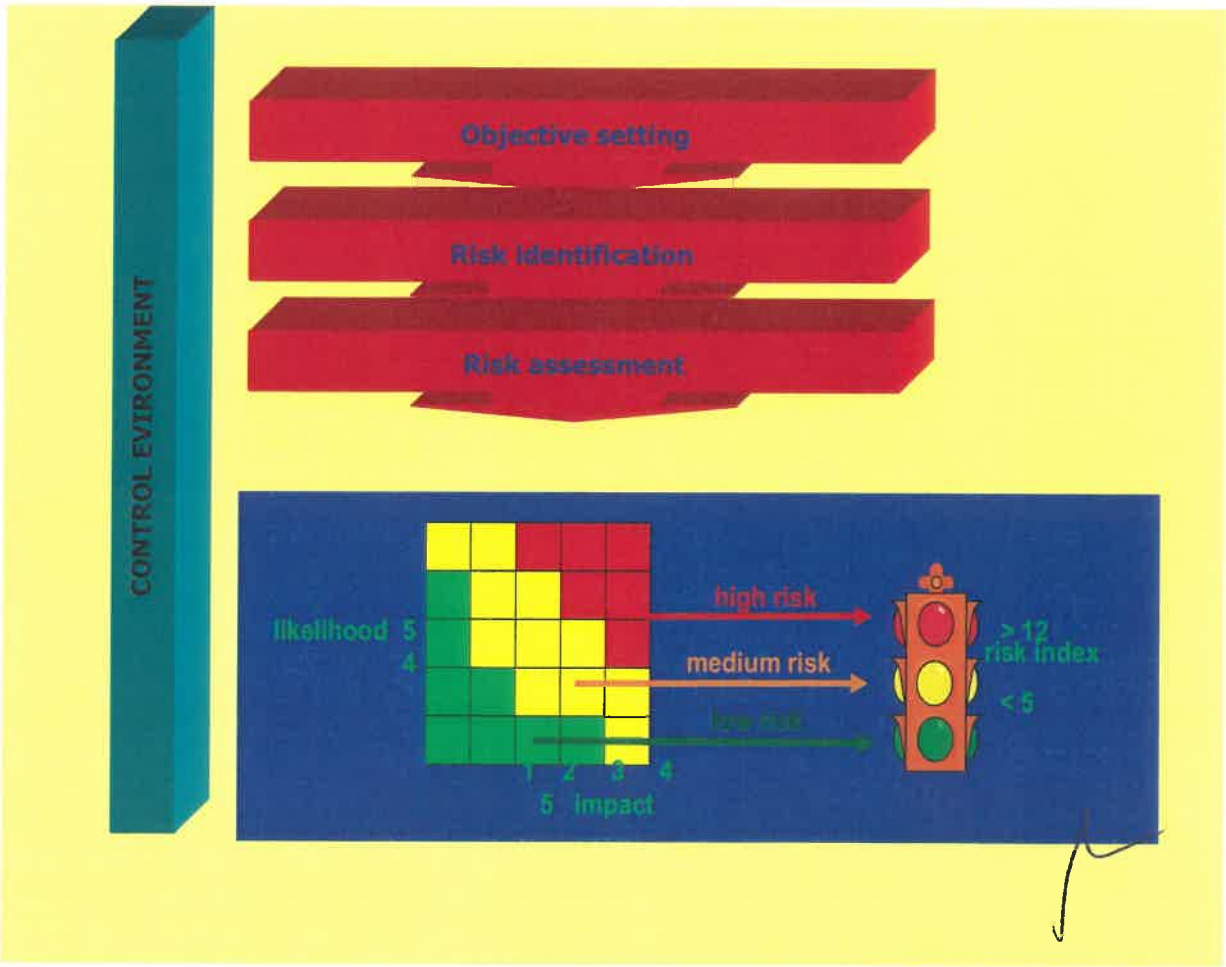
(1) Exposure = Total Rand-value at risk without regard to the probability for negative events.

4.2.2 Focus on the asset at risk (what was put to work by management)? Consider the size, type, probability and location. Think of what can be exposed e.g. people, money, assets, intellectual property, business name and reputation, going concern, individual reputation, embarrassment and other. Note that all the above are internal risks for which the department has direct control thereupon.

4.2.3 **Specific inherent risks**: it covers the following; Competence of employees, Complexity of business, adequacy of information systems and activity specific

5. RISK ASSESSMENT

The department will establish the RM Committee to drive the risk management processes.



Risk Rating Tables

Impact

The following is an example of a rating table that can be utilised to assess the potential impact of risks. Institutions are encouraged to customise the rating table to their specific requirements.

Rating	Assessment	Definition
1	Insignificant	There is 90-100% that the objective will certainly be achieved. **(Acceptable- No action required)**
2	Minor	There are 70-89% chances that it is likely that the objective will be achieved. **(Mostly acceptable- Low level of control intervention required, if any)**
3	Moderate	There are 50-69% chances that it is likely that the objective will be achieved. **(Moderate level of control intervention required)**
4	Major	There are 30-40% chances that it is likely that the objective will be achieved. **(Unacceptable level of risk- Major level of control intervention required)**
5	Critical	There is 1-29% that it is likely that the objective will be achieved. **(Unacceptable- Action must be taken immediately)**

Likelihood

The following is an example of a rating table that can be utilised to assess the likelihood of risks. Institutions are encouraged to customise the rating table to their specific requirements.

Rating	Assessment	Definition
1	Rare	The risk is conceivable but is only likely to occur in extreme circumstances
2	Unlikely	The risk occurs infrequently and is unlikely to occur within the next 12 months
3	Moderate	There is an above average chance that the risk will occur at least once in the next 12 months
4	Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months
5	Common	The risk is already occurring, or is likely to occur more than once within the next 12 months

Inherent risk exposure (impact x likelihood): Residual risk exposure (inherent risk x control effectiveness)

The following is an example of a rating table that can be utilised to categorise the various levels of inherent risk. Institutions are encouraged to customise the rating table to their specific requirements.

Risk rating	Risk magnitude	Response
20 - 25	Maximum	Unacceptable- Action must be taken immediately (0-3 months)
15 - 19	High	Unacceptable level of risk, except under unique circumstances or conditions - Major level of control intervention required to achieve an acceptable level of residual risk (3-6 Months)
10 - 14	Medium	Unacceptable level of risk, except under unique circumstances or conditions - Moderate level of control intervention required to achieve an acceptable level of residual risk (6-12 Months)
5 – 9	Minimum	Mostly acceptable - Low level of control intervention required, if any
1 – 4	Low	Acceptable-No action required

Impact and likelihood

LIKELIHOOD	5	Frequent	5	10	15	20	25
	4	Likely	4	8	12	16	20
	3	Moderate	3	6	9	12	15
	2	Unlikely	2	4	6	8	10
	1	Rare	1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Critical
	Rating		1	2	3	4	5
	IMPACT						

6. CONTROL ASSESSMENT

6.1 LISTING OF CONTROLS

6.1.1 Where there are already controls in existence, those controls will be listed and rated using the same criteria as used with the risk rating (estimates).

6.2 ASSESSMENT OF CONTROLS AND THE INTERNAL AUDIT STRATEGY

6.2.1 According to your assessment, rate the controls between 1 and 25 according to how much of the risk does the control eliminate. When you subtract the control rating from the risk rating, the remainder is your residual risk. This exercise is called the control self assessment process

6.2.2 After the assessment has been finalised, the risks with high residual values or those that have never been treated should be prioritised by owners. Action Plans will be drawn up with deadlines and follow up dates. If management prefer, the PIA (Provincial Internal Audit) would be tasked with a responsibility to assist management to deal with the risk.

6.2.3 The output of both the risk assessment and control assessment is the Risk Registers for the CRO and the management, and the Internal Audit Plans for the PIA.

7. RISK MANAGEMENT STRATEGIES

7.1 Exposure falls into two types, risk control and risk financing. Risk control techniques prevent or reduce the frequency or severity of losses. Risk financing techniques, e.g. retention, insurance, and non-insurance transfers of financial obligations, pay for those losses that occur despite the best risk control efforts. Risk control strategies are categorised as follows:

7.1.1 Risk Avoidance – this approach simply means that the department does not undertake an activity, action or programme that would produce an undesirable loss exposure.

7.1.2 Risk Prevention – this technique focuses on reducing the frequency of losses. E.g. frequent inspections of an office for overload of electrical outlets are a fire prevention technique.

7.1.3 Risk Reduction – based on the assumption that "it is not feasible" or "it is

impossible" to eliminate or prevent an exposure, this method serves to minimise occurrence, e.g. the use of a sprinkler system will reduce the amount of damage from the fire.

7.1.4 Segregation of Exposures – with this approach, the department 's activities and programmes may be separated, diversified, or duplicated so a single risk will not cause a catastrophic loss to all, e.g. storing supplies in several different locations instead of one large warehouse, diversifying cash assets, and backing up all computer data and storing off-site.

7.1.5 Risk Transfer – transferring, normally through a contract, the financial and or legal liabilities associated with an identified risk to an outside organization e.g. a building lease, as opposed to ownership of a building, transfers certain risk exposures from the lessee to the lessor, or the owner of the building. It is noted that insurance policies of the department are being reviewed in order to determine the department's financial protection against an undesirable event or risk

Please take note that our risk appetite/acceptable level will help us determine which risk management strategy to use to address a specific risk.

8. OTHER CONTROLS THE DEPARTMENT WILL USE TO MITIGATE RISK

8.1 Develop concise, written policies and procedures – the department shall carefully write up-to-date employee policies which will provide a thorough explanation of its rules. Policies and Procedures are an organization's first and best defence against employment-related disputes.

8.2 Provide a back up for performance of each key role – another person in the department will have a general understanding of another person's role in case that other person for some reason is not able to perform the role.

8.3 Institute sound general financial management and accounting controls – the creation of adequate accounting controls will focus on authority and approval, proper documentation, physical security, and early detection of non-conformance.

8.4 Institute security safeguards to protect the inadvertent release of confidential information – these safeguards will include a well thought out security policy, security training, and security management and maintenance.

8.5 Establish ongoing educational programmes – conduct seminars for staff in such areas as safety, sexual harassment, confidentiality, etc. and maintain records of these educational activities.

8.6 Use a variety of other preventive activities – such activities will include a client relations programme, an employee newsletter, a formal safety and security programme, a community input effort, and ongoing planning, coordination, and function review and client surveys (customer feedback)

9. COMMUNICATION AND REPORTING

9.1 Effective and continuous monitoring is an essential part of risk management and therefore relevant. Stakeholders will receive reports pertaining to the current status of financial and operational data supported by adequate and appropriate systems. This will be within a time frame that enables the staff to carry out their responsibilities properly.

9.2 Awareness campaigns will be detailed together with an analysis of previously conducted campaigns. Continuous evaluation of this form of communication will ensure development of campaigns that achieve the desired results.

9.3 The reason for communicating and documenting is for staff to understand the risks and mitigation alternatives as well as the risk data to make effective choices within the constraints of available resources. Communication and documentation are both critical for managing risks. Information both positive and negative, when communicated throughout the organisation, will ensure that best practice is used and understood.

9.4 Training is another important method of communication where practical skill transfer courses will be upheld on an ongoing basis. Staff will understand what is expected of them and be able to proactively identify, evaluate and implement solutions to risk.

9.5 Reports to the Audit Committee and to the management will provide a balanced assessment of significant risks and the effectiveness of risk management process in managing those risks. Any major weakness that has been identified will be noted together with any possible impact and actions being taken to rectify them. It is essential that there be an open communication between management and the Audit Committee.

9.6 The Audit Committee will advise what changes, if any, can be made regarding the risk management process. These changes may be due to:-

9.6.1 Non-achievement of objectives;
9.6.2 Lack of flexibility in responding to changes in the internal and external Environments;
9.6.3 The coverage and quality of risk management plan;
9.6.4 Ineffective risk identification, communication and reporting;
9.6.5 Commitment to continuous improvement.

9.7 The reason the responsible Executive Authority will satisfy itself with regard to the effectiveness of risk management is that in the annual report it will account for how the organisation has dealt with the risk and provide a statement that indicates the executive authorities' responsibility for risk management. The statement will indicate;

9.7.1 How a risk management culture is being cultivated;
9.7.2 How the appropriate infrastructure is being established;
9.7.3 Management's commitment to:
  i. Strive for continuous risk management training to enable effective communication
  ii. Reinforcement of risk management processes through human resource mechanisms
9.7.4 The levels of unacceptable risk both financially and reputational.
9.7.5 The manner and frequency in which significant risks are reported.

10. Monitoring and Review process- chief risk officer

10.1 The monitoring and review of the process assists in tracking the changes within risk management and the effectiveness of the plan. An important component of risk management plan is identifying benchmarks that will determine management commitment and the effectiveness of risk management procedures. Monitoring of risks will be linked to the organisation's key performance indicators which are in turn linked to organisational objectives. Programme directors will have risk management as a key performance area. Monitoring will promote a reporting structure that is accurate and allow for the objective evaluation of internal controls.

11. RISK MANAGEMENT STRUCTURE

11.1 For risk management to be integrated and effective in the department the structure needs to report to the Head of the Department.

11.2 The Chief Risk Officer (CRO) will coordinate risk management processes, monitor risk registers and table a report on the status of risk management in all Departmental Committee Meetings (EMC & DMC) and Risk Management Committee Meetings (RMC).

12. PERIOD OF REVIEW AND AMENDMENT

This strategy shall be reviewed annually and in the event of any need for amendments, such amendments shall be made and affected to the strategy.

Recommended by the Risk Management Committee:

Signature: _____

Date: 09/04/2018

Approved by the Accounting Officer / Authority:

Signature: _____

Date: 17/4/2018

ANNEXURE A: RISK MANAGEMENT IMPLEMENTATION PLAN

Planned Action	Detailed Actions	Outputs	Due date and responsible person	Progress to date
Risk orientation				
Review the risk management policy	Risk Management Committee (RMC) to review the policy and recommend to the Accounting Officer / Authority for approval.	Approved risk management policy	Chief Risk Officer 29/06/2018	
Risk orientation				
Review the risk management strategy	Develop guidelines on roles and responsibilities for risk management committee (RMC) to review the strategy and recommend to the Accounting Officer / Authority for approval	Approved risk management strategy	Chief Risk Officer 29/06/2018	
Publication of Risk Management Policy & Strategy	Publicize the policy on the intranet	Communicated risk management policy & strategy to all officials in the Department	Chief Risk Officer 29/06/2018	

Planned Action	Detailed Actions	Outputs	Due date and responsible person	Progress to date
Raising awareness and risk management training	Develop and formalise detailed training programme/ plan for all officials Develop risk orientation programme for new employees.	Completed orientation for all officials and RMC members. Make presentations on risk management at management meetings.	Chief Risk Officer RMC Chairperson 29/06/2018	
Terms of reference for the Risk Management Committee	Review existing RMC's Terms of Reference and align to the RM strategy.	Approved risk management committee charter	Chief Risk Officer 29/06/2018	
Risk assessment				
Facilitate enterprise-wide risk assessments.	Facilitate risk identification and assessment sessions. Analyse information and develop risk assessment reports.	Approved strategic risk register. Approved operational risk register.	Chief Risk Officer Senior managers Other officials 30/04/2018 31/07/2018	

Planned Action	Detailed Actions	Outputs	Due date and responsible person	Progress to date
Risk response				
Develop risk response strategies	Drafting action plans for all gaps identified in addressing the risks.	Strategic & Operational Risk Registers	Risk Owners 30/04/2018 31/07/2018	
Risk monitoring				
Assess risks controls effectiveness	Assign assurance providers to assess the controls of all the risks identified (monitored risks).	Risk Monitoring Report	Chief Risk Officer All Managers Quarter 3 & 4	
Facilitate the execution of ERM processes and infrastructure.	Implement appropriate risk reporting to the Accounting Officer, Executive Authority, Audit Committee, RMC, DMC, EMC and Provincial Risk Management Forum.	Approved progress reports: present progress reports to various stakeholders at various intervals.	Chief Risk Officer Quarterly	