KZN DEPARTMENT OF PUBLIC WORKS

RISK MANAGEMENT STRATEGY

TABLE OF CONTENTS

1. INTRODUCTION

Risk management is a central part of any organization's strategic management. It is the process whereby an organization both methodically and intuitively addresses the risk attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of activities.

Risk management is recognized as an integral part of sound organizational management. Risk management in the public sector derives its mandate from the Public Finance Management Act (PFMA).

2. GENERAL RESPONSIBILITIES OF THE ACCOUNTING OFFICER

With regard to the Risk Management, The Public Finance Management Act stipulates in Section 38 that the Accounting Officer for a department:

a) must ensure that the department has and maintains:

i) Effective, efficient and transparent systems of financial and risk management and internal control;

ii) A system of internal audit under the control and direction of an audit committee complying with and operating in accordance with regulations and instructions prescribed in terms of section 76 and 77;

iii) An appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost effective;

iv) A system for properly evaluating all major capital projects prior to a final decision on the project

b) is responsible for the effective, efficient, economical and transparent use of resources of the department;

c) must take effective and appropriate steps to:

i) collect all money due to the department

ii) prevent unauthorised, irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct; and

iii) manage available working capital efficiently and economically;

d) is responsible for the management, including the safeguarding and the maintenance of the assets, and for management of the liabilities of the department;

e) must comply with any tax, levy, duty, pension and audit commitments as may be required by legislation;

f) must settle all contractual obligations and pay all money owing, including intergovernmental claims within the prescribed or agreed period;

g) on discovery of any unauthorised, irregular or fruitless and wasteful expenditure must immediately report , in writing, particulars of the expenditure to the relevant treasury and in the case of irregular expenditure involving procurement of goods or services;

h) must take effective and appropriate disciplinary steps against any official in the service of the department who:

i) contravenes or fails to comply with the provisions of the Act;

ii) commits an act which undermines the financial management and internal control system of the department;

iii) makes or permits an unauthorised expenditure, irregular expenditure or fruitless and wasteful expenditure;

The extension of the general responsibilities, in terms of Section 45 of the PFMA, to all managers is a cornerstone in the institutionalization of risk management in the public service. It establishes responsibility for risk management at all levels of management, extending it beyond the roles of the Accounting Officer and the Internal Audit units or the Audit Committee.

The roles and responsibilities for the implementation of a Risk Management strategy is contained in the Treasury Regulations published in terms of the PFMA. Section 3.2 of the regulations revolves around risk management and can be summarized as follows:

- *The Accounting Officer must ensure that a risk assessment is conducted regularly to identify emerging risks for the institution.*
- *The risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority and to determine the skills required of managers and staff to improve controls and to manage these risks.*
- *The risk management strategy must be clearly communicated to all officials to ensure that it is incorporated into the language and culture of the institutions, and embedded in the behavior and mindset of its people.*

3. RISK MANAGEMENT COMMITTEE

As an additional measure, The Accounting Officer of KZN Department of Public Works has established the:

3.1. Head Office Risk Management Committee comprising of the following members:

- Head of Department;
- Chief Financial Officer;
- General Manager: Operations;
- General Manager: Property Management;
- General Manager: Corporate Services;
- Head of Ministry;
- Manager: Security;
- Manager: Legal Services;
- Manager: Compliance and Risk Management.

Other parties who may be requested to attend include:

- Auditor General;
- Provincial Internal Audit Unit;
- Parties appointed to carry out audits and forensic investigations;

3.2. Regional Office Risk Management Committees comprising of the following members:

- Regional Manager
- Regional Operations representative
- Regional Real Estates representative
- Regional Finance representative
- Regional Corporate Services representative
- Regional Security Services representative
- Regional Supply Chain Management representative
- Manager: Compliance & Risk Management
- Deputy Manager: Risk Management
- Deputy Manager: Compliance

Ad Hoc requests may be made for relevant functional units not mentioned above to provide insight/clarity/expertise when required.

3.3. The responsibilities of the Risk Management Committee will be the following:

- The process of Risk Management;
- Review the processes and procedures for risk identification, analysis and qualification;
- Ensure an effective, ongoing process is in place to identify risks, measure their impact and proactively manage and monitor them;
- Ensure the review of the risks profile annually and review reports on risk management progress;
- Review reports from external and internal audit on the effectiveness of the processes and procedures of risk and internal control and
- Ensure that reports are being acted upon and followed up.

The Head Office Risk Management Committee will meet at least four times a year ie quarterly and the Regional Risk Management Committees will meet bi-monthly

4. THE KING REPORT

The King report on Corporate Governance also reflects on risk management as an integral part of strategic and operational activities wherein Corporate governance can, be viewed as a strategic response to prudent risks, in exchange for measurable rewards.

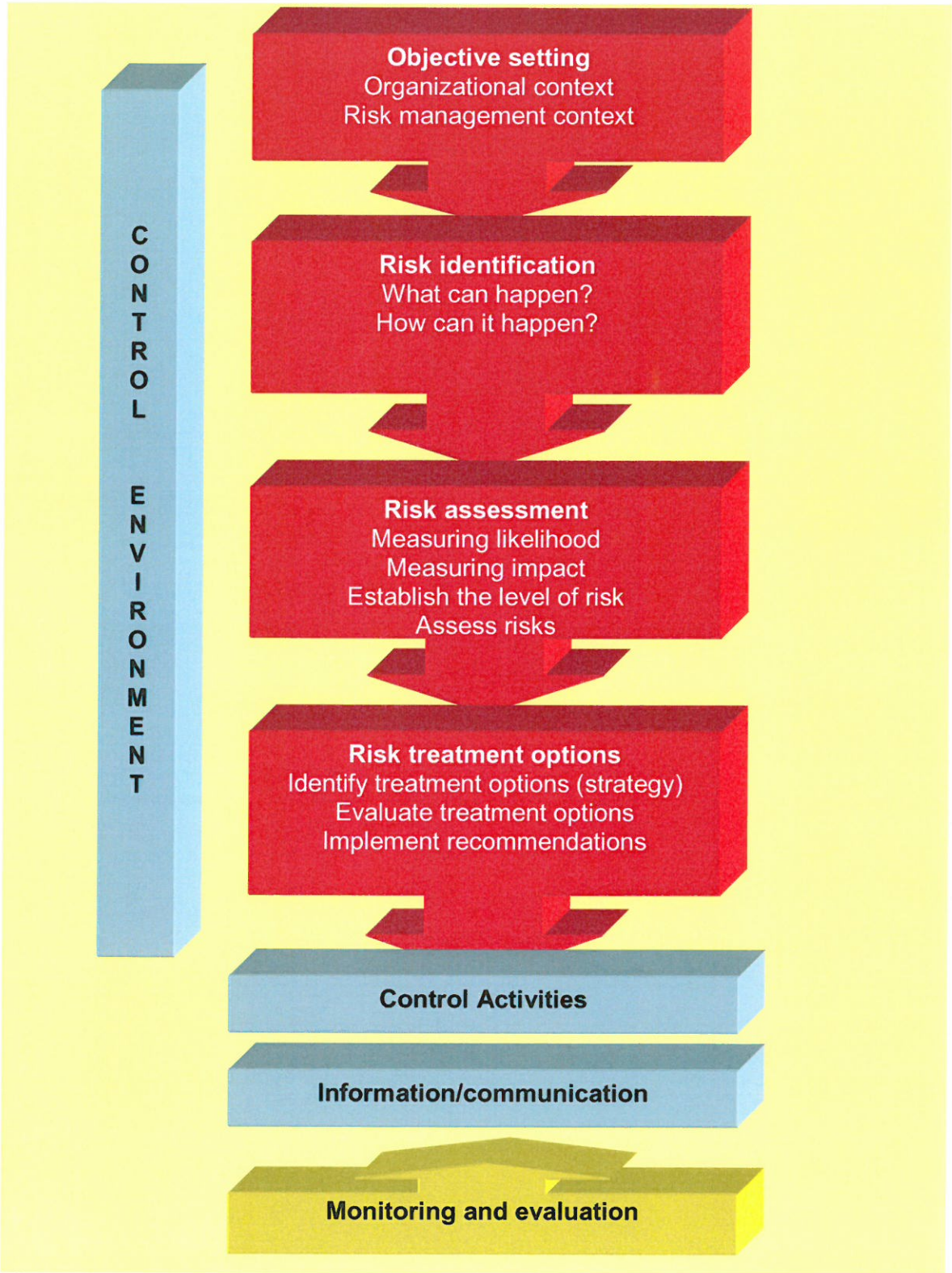
5. COSO

The Risk Management Strategy of the KZN Department of Public Works is derived from the COSO (best practice model) Risk Management model. The model stipulate the following interrelated components:

- Control environment;
- Objective setting;
- Risk identification;
- Risk assessment;
- Risk management strategy;
- Control activities;
- Information and communication; and
- Monitoring.

The following table indicates the different relationships between the components:

Eight components of risk management



The components are described as follows:

6. RISK MANAGEMENT STRATEGY

6.1 Control environment

The KZN Department of Public Works' control environment is the foundation of risk management, providing discipline and structure. The control environment influences how strategy and objectives are established, department activities are structured, and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities.

The KZN Department of Public Works shall at all times, promote a positive control environment, which comprise amongst others the entrenchment of ethical values, competence building and development of personnel, proper delegations of authority and responsibility.

The KZN Department of Public Works will further entrench risk management as part of the strategic and daily operations of the department. Risk tolerance level shall be set for each key activity during the strategic planning process.

A code of conduct, policies and procedures shall be communicated to all staff members and action taken against those who fail to comply with the set policies and the code of conduct.

A performance management system shall be put in place and implemented. Such a performance management system shall include the assessment of management on risk management.

The KZN Department of Public Works shall conduct a control environment survey once in every three years. The survey shall assess, amongst others the following:

- Risk Management philosophy and culture
- Integrity and ethical values
- Organisational structure (planning, executing, control and monitoring)
- Delegation of authority and responsibility
- Committed to comply with Acts, policies and procedures.
- Staff competency
- Strategic Planning processes, etc

6.2 Objective Setting

Objectives must exist before management can identify events potentially affecting their achievement. Risk management ensures that management has a process in place to both set objectives and aligns the objectives with the department's mission/vision and is consistent with the department's risk tolerance. The setting of these objectives is usually completed during the, "Strategic planning and Budgetary process."

Department objectives can be viewed in the context of the following five categories:

- **Strategic** – relating to high-level goals, aligned with and supporting the department's mission/vision;
- **Operations** – relating to effectiveness and efficiency of the department's operations, including performance and service delivery goals.
- **Reporting** – relating to the effectiveness of the department's reporting. They include internal and external reporting and may involve financial or non-financial information;
- **Compliance** – relating to the department's compliance with applicable laws and regulations;
- **Safeguarding of assets** – relating to prevention of loss of the Department's assets or resources, whether through theft, waste or inefficiency. Safeguarding of assets also include the prevention or timely detection of unauthorized acquisition, use, or disposition of the department's assets.

This categorization of department objectives allows management and the executive authority to focus on separate aspects of Risk Management.

Risk and exposures shall be identified in the formulation of objectives.

6.3 Risk identification

Internal and external events and/or factors affecting achievements of the KZN Department of Public Works' objectives must be identified, distinguished between those with negative and positive impact. Events or factors with a positive impact must be channeled back to management strategy or objective setting processes. During this identification phase, all financial and non-financial factors that may influence the Department's policy and management agenda must be identified.

The Department's risk identification methodology shall comprise a combination of techniques and supporting tools. Risk identification techniques shall look to both the past and the future.

The following methods shall amongst others, be used either individually or collectively to identify risks and exposures:

- interview/focus group discussion;
- audits or physical inspections;
- brainstorming;
- Survey, questionnaire;
- Judgmental – speculative, conjectural, intuitive;
- History, failure analysis;
- Examination of personal experience or past department or public entity experience;
- Incident, accident and injury investigation;
- Scenario analysis;
- Decision trees;
- Strengths, weaknesses, opportunities, threats (SWOT) analysis;
- Flow charting, system design review, systems;
- Work breakdown structure analysis; and
- Operational modeling.

The following are some of the key questions that shall be used in identifying and controlling the risks

- What, when, where, why and how risks are likely to occur, and who might be involved?
- What is the source of each risk?
- What are the consequences of each risk?
- What controls presently exist to mitigate each risk?
- To what extent are controls effective?
- What alternative, appropriate controls are available?
- What are the department obligations – external and internal?
- What is the need for research into specific risks?
- What is the scope of this research, and what resources are required?
- What is the reliability of the information?
- Is there scope for benchmarking with peer organizations?

6.4 Risk Assessment

Risk assessment is a formal and a systematic approach to conduct a detailed examination and evaluation of the Departmental risks and exposures. Risk assessment shall focus on all significant areas of impact relevant to the Department or its activities. In this phase, risks are assessed, considering their likelihood and impact, as a basis for determining how they should be managed. Risks shall be assessed on both an inherent and residual basis.

The Department shall conduct a risk assessment at least once in every three years and review the risks profile annually.

The risk assessment process shall include the following 4 steps:

Step 1: Quantifying the parameters (scoring system) of impact and likelihood before the actual assessment (see tables below);

IMPACT (CONSEQUENCE)		
Score	**Rating**	**Description**
5	Catastrophic	• Loss of ability to sustain ongoing operations. • Leads to termination of the project
4	Major	• Significant impact on achievements of strategic objectives and targets relating to the organizational plan. • Cost increase > 20%
3	Moderate	• Disruption of normal operations with limited effect on achievement of strategic objectives or target relating to the organizational plan • Cost increase > 10%
2	Minor	• No material impact on achievement of the organization's strategic objectives • Cost increase < 10%
1	Insignificant	• Negligible impact • Minimal or no impact on cost

LIKELIHOOD (FREQUENCY, PROBABILITY)		
Score	**Rating**	**Description**
5	Common	The risk is almost certain to occur more than once within the next 12 months/ almost every time (Probability = 100% p.a)
4	Likely	The risk is almost certain to occur once within the next 12 months (Probability = 50 – 100% p.a)
3	Moderate	The risk could occur at least once in the next 2-10 years (Probability = 10-50% p.a)
2	Unlikely	The risk could occur at least once in the next 10-100 years. (Probability = 1-10% p.a)
1	Rare	The risk will probably not occur –less than once in 100 years. (Probability = 0-1%)

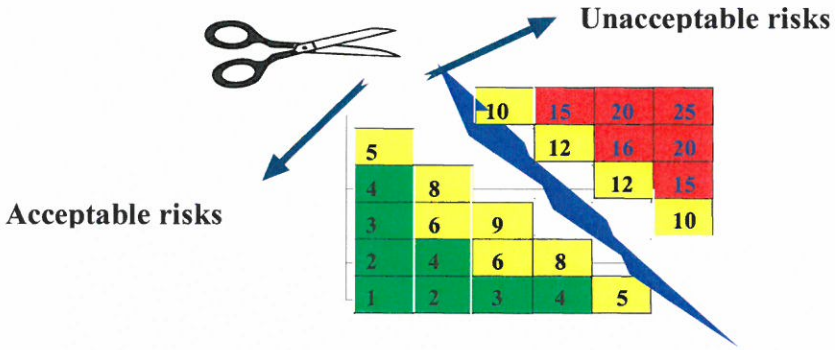
Step 2: Applying the parameters to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium or low risk (see tables below);

Risk index = impact x likelihood

I	5	5	10	15	20	25
M	4	4	8	12	16	20
P	3	3	6	9	12	15
A	2	2	4	6	8	10
C	1	1	2	3	4	5
T		1	2	3	4	5
		LIKELIHOOD				

Risk index	Risk Magnitude
20 - 25	Maximum
15 - 19	High risk
10 - 14	Medium risk
5 - 9	Low risk
1 - 4	Minimum risk

Step 3: Determining the risk acceptance criteria by identifying what risks will not be tolerated (see table below);



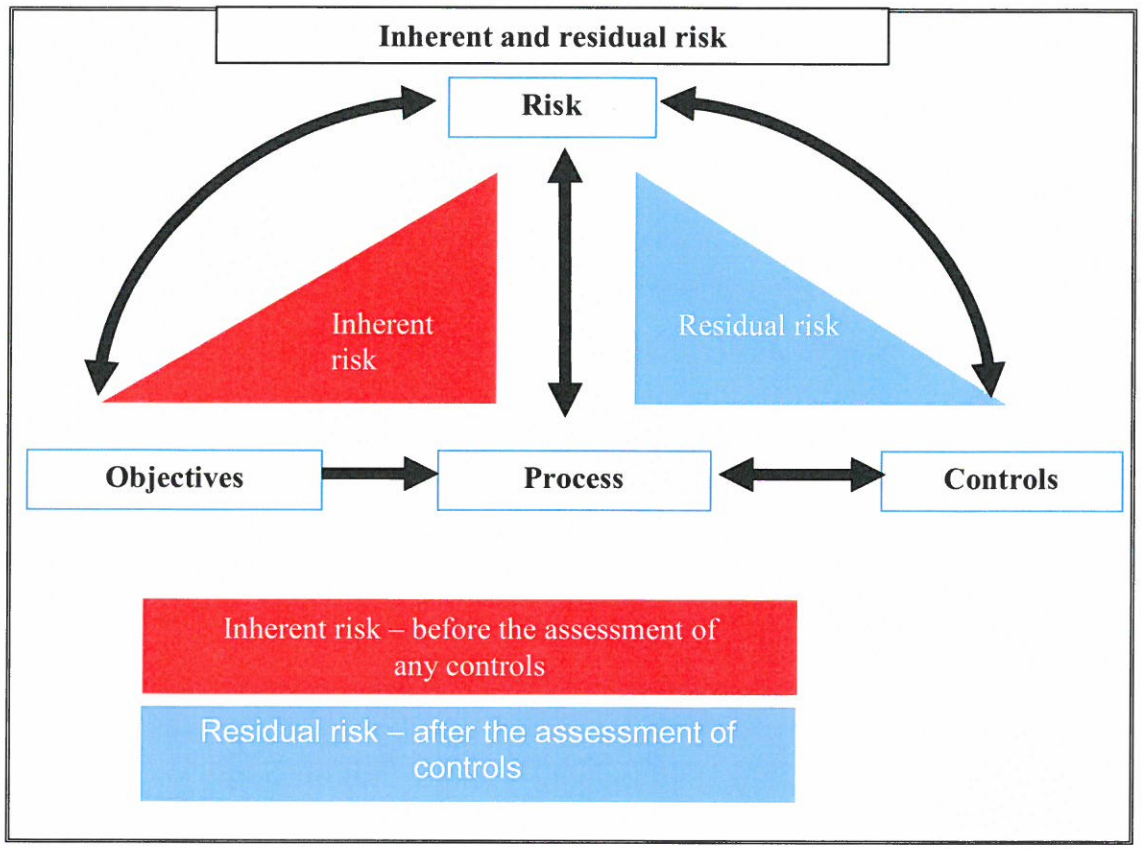
Step 4: Determine risk acceptability and what action will be proposed to reduce the risk (see table below).

Risk index	Risk magnitude	Risk acceptability	Proposed actions
20 – 25	Maximum risk	Unacceptable	Take action to reduce risk with highest priority, Accounting Officer and executive authority attention.
15 – 19	High risk	Unacceptable	
10 – 14	Medium risk	Unacceptable	Take action to reduce risk, inform senior management.
5 – 9	Low risk	Acceptable	No risk reduction - control, monitor, inform management.
1 - 4	Minimum risk	Acceptable	No risk reduction - control, Monitor, inform management.

Likelihood represents the possibility that a given event will occur, while impact represents its effect should it occur.

The rating of the risks shall be conducted through a voting system. Risk shall be rated both on inherent and residual basis. Residual risk represents risk after considering the effectiveness of existing control.

The following diagram differentiates between inherent and residual risk:



6.5 Risk treatment options

Management identifies risk management strategy options, which should include a fraud prevention plan, and consider their effect on event likelihood and impact, in relation to risk tolerances, costs versus benefits, and thereafter designs and implements response options. The consideration of risk management strategies and selecting and implementing a risk response plan is integral to risk management and requires that management select a response that is expected to bring risk likelihood and impact within the Department's risk tolerance level.

Risk Management Response plan or treatment options shall be classified under the following broad categories:

- **Risk Avoidance**. A decision not to be involved with a risk or in a risk situation. The decision will be not to proceed with a particular activity or project because upon assessment, the activity represents such a great risk that there is limited ability to control the risk and that there is little benefit in pursuing the activity.

- **Risk Control** – Is the pro-active control of adverse consequences of a risk by implementing preventative measures. It is the risk, which is cost effective to control or treat.

- **Risk Transfer/sharing** – It is the risk that upon assessment shall be considered cost effective to transfer to third parties or otherwise sharing a portion of the risk with the third party.

- **Risk Retention** – It is the risk that upon assessment shall be considered cost effective to be accepted or tolerated due to its limited impact on the Department.

The response plan shall be developed once the risk assessment has been completed and shall include all the intervention to minimize the identified risks.

6.6 Control Activities

Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly and in a timely manner. Control activities are part of the process by which a department strives to achieve its business objectives.
Control activities refer to policies, procedures, processes and systems that the Department maintains to minimize risks and exposures and ensure that risk management strategies are properly executed.

Control activities shall involve two elements: a policy establishing what should be done and procedures to affect the policy.

6.7 Broad internal control focus areas

Internal controls established in a department should focus on the following areas:

- **Adequate segregation of duties**

Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions and events should be separated among individuals;

- **Custody and accountability for resources**

Access to resources and records are to be limited to authorized individuals who are accountable for their custody or use;

- **Prompt and proper recording and classification of transactions**

To ensure that information maintains its relevance and value to management in controlling operations and decision-making and to ensure that timely and reliable information is available to management;

- **Authorization and execution of transactions**

Requires that employees execute their assigned duties in accordance with directives and within the limitations established by management or legislation;

- **Documentation**

Internal control structures, i.e. policies and procedures, and all transactions and significant events are to be clearly documented;

- **Management supervision and review**

Competent supervision is to be provided, including assignment, review and approval of an employee's work.

Employees should be provided with the necessary guidance and training to help ensure that errors, wasteful, and wrongful acts are minimized and that specific management directives are understood and achieved.

6.8 Computer controls should be geared towards the following areas:

- **Access controls**

Controls should be designed to prevent:

- Unauthorized changes to programs which process data;
- Access to files which store accounting and financial information and application programs;
- Access to computer operating systems and system software programs;
- User-id's and passwords should be used to limit access to programs, data files and software applications;
- Firewalls should be installed to prevent data corruption from unauthorized external access.
- Computer Operating system: Controls should be designed to manage the operation of the system and to ensure that programmed procedures are applied correctly and consistently during the processing of data.

  Computer controls such as scheduling of processing time, execution of programs by competent personnel, monitoring and review of the function of hardware, division and rotation of duties and maintenance of system and manual logs with regular follow-up management should be available.

- **System Software Programs**

Controls should be designed for programs, which do not process data to ensure that they are installed or developed and maintained in an authorized and effective manner, and that access to system software is limited.

This could be achieved through security over system software, database systems, networks and processing by users on personal computers. There should be support structures, error correction methods and adequate documentation for the systems.

Controls should be designed to ensure the continuity of processing, by preventing system interruption or limiting this to a minimum.

Controls that should be in place include physical protection against the elements such as fire, water and power. There should be emergency plan and disaster recovery procedures, provision of alternative processing facilities, backups of data files, maintenance of hardware, adequate insurance, cable protection, uninterruptible power supply, prevention of viruses and personnel controls affecting security and continuity.

- **Information systems controls**

With widespread reliance on information systems, controls are needed over significant systems. Two broad groupings of information systems control activities can be used. The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation. The second is application controls, which include computerized steps within application software to control the technology application. Combined with other manual process controls where necessary, these controls ensure completeness, accuracy and validity of information.

General controls include controls over information technology management, which will address the information technology oversight process, monitoring and reporting information technology activities, and department improvement initiatives. Other controls include information technology infrastructure, security management and software acquisition, development and maintenance. These controls apply to all systems from mainframe to client/server to desktop computing environments.

Application controls are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing. Individual applications may rely on effective operation of controls over information systems to ensure that interface data are generated when needed, supporting applications are available and interface errors are detected and corrected timeously.

Because each department has its own set of objectives and implementation approaches, there will be differences in objectives, structure and related control activities. Even if two departments had identical objectives and structures, their control activities would likely be different, as different people who use individual judgements in effecting internal control manage them. Moreover, controls reflect the environment and industry in which a department operates, as well as the complexity of its department, its history and its culture.

6.9 Information and Communication

Relevant information – both from internal and external sources, financial or non-financial – must be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the department, as well as the exchange of relevant information with external parties, such as customers, suppliers, regulators and shareholders.

Information shall be provided to all levels of a department to identify, assess and respond to risks, and to otherwise run the department and achieve its objectives

An information system infrastructure shall be established to source, capture, process, analyze and report relevant information.

Management must keep the executive authority up-to-date on performance, developments, risks and the functioning of risk management, and other relevant events and issues. The more effective the communication, the more successful the executive authority will be in carrying out its oversight responsibilities, in acting as a sounding executive authority on critical issues and in providing advice, counsel and direction. By the same token, the executive authority should communicate to management what information it needs and provide feedback and direction.

Communication should raise awareness about the importance and relevance of effective risk management, communicate the department's risk tolerance levels, implement and support a common risk language, and advise personnel of their roles and responsibilities in effecting and supporting the process of risk management.

6.10 Monitoring

Risk management shall be regularly monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time.

Monitoring shall be done in two ways: through ongoing activities and separate evaluations. This will ensure that risk management continues to be applied at all levels and across the department.

Ongoing monitoring is built into the normal, recurring operating activities of a department, is performed on a real-time basis and reacts dynamically to changing conditions and is ingrained in the department. Management must assess the effectiveness of controls or a chosen risk treatment option.

Since separate evaluations take place after the fact, separate evaluation shall be conducted by the Internal and External Auditors. The Internal audit plan shall be risk based and high-risk areas shall be prioritized. Internal Audit provides assurance to management that internal controls, risk management and governance processes are in place and functioning effectively. The External Auditors or Office of the Auditor-General shall perform independent reviews of internal controls, risk management and governance processes.

7. STRATEGY IMPLEMENTATION

This strategy shall upon approval, be communicated to all staff members.

The Risk Committees shall be responsible for monitoring implementation of the Risk management strategy and the Directorate: Compliance & Risk Management shall be further responsible to facilitate the implementation of the Risk management strategy.

8. APPROVAL OF THE STRATEGY

The Risk Management Strategy, and any amendments thereto, become effective upon approval by the Accounting Officer of the Department of Public Works or his/her delegated official.

Approved on the 17th day of JUNE 2014 at Pietermaritzburg.

_____

THE ACTING HEAD: KZN DEPARTMENT OF PUBLIC WORKS