DCSR POLICY: ENTERPRISE RISK MANAGEMENT STRATEGY AND FRAMEWORK

DOCUMENT INFORMATION AND LOG

File Name	**Enterprise Risk Management Strategy And Framework**
Original Author	**Department Of Culture Sport And Recreation**
Review Date	**2025**

FOREWORD

This is Mpumalanga Department of Culture, Sport and Recreation's Enterprise Risk management Strategy and Framework. This strategy aims to improve the effectiveness of risk management across the department. This is a high level plan which outlines how the department will go about implementing its risk management policy and plan.

Effective risk management allows us to:

a) Have increased confidence in achieving our priorities and outcomes.
b) Constrain threats to avoidable risks.
c) Take informed decisions about exploiting opportunities.
d) Ensure that we get the right balance rewards and risks.
e) Improve our partnership working arrangements and corporate governance.
f) Ultimately, effective risk management will help to ensure that the department maximizes its opportunities, and minimizes the impact of risks it faces, thereby improving our ability to deliver our priorities and improve outcomes for farmers.

This risk management strategy explains the department's approach to risk management and the framework in which we operate to ensure that we manage our risks effectively.

The department is committed to effective management of risks. The department's employees, stakeholders, assets and ability to deliver services to the farmers of Mpumalanga are constantly affected by such risks. The department recognizes that its risks need to be managed so that pitfalls are avoided, but opportunities are not missed.

Our risk management philosophy is, **"We are all risk managers"**.

Contents

Glossary of terms

Throughout this document, unless otherwise stated, the words in the first column below have the meanings stated opposite them in the second column (and cognate expressions shall bear corresponding meanings):

Terminology	Definition of terminology
Risk	An unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such Opportunities.
Risk Management	'Risk Management is *a* systematic process to identify, evaluate and address risks on a continuous basis before such risks can impact negatively on the institution's service delivery capacity"
Risk Assessment	The overall process of identifying, analyzing and evaluating risk. The risk assessment process should consider risks that are significant to the achievement of the Department's objectives. This is a continuous process, requiring regular reviews, as and when internal and external changes influence the Department's strategies and objectives.
Enterprise Risk Management (ERM)	Enterprise Risk Management is a structured and consistent approach across the Department that aligns strategy, processes, people, technology and knowledge with the purpose of evaluating and managing the risks (threats and opportunities) that the Department faces to create stakeholder value Or

	Choices made under conditions of uncertainty, bound by acceptable levels of risk, designed to sustain/ maximize stakeholder value.
Inherent Risk	The product of the likelihood and impact (Risk before consideration of current control effectiveness). **Inherent risks within processes considering the nature of processes.**
Interdepartmental risks	Risks that should be shared between various departments and managed collectively.
Residual Risk	The level of risk faced by the Department after considering the effectiveness of existing controls and their perceived effectiveness.
Risk Mitigation	The process of selecting and implementation measures to modify risk (encompasses risk avoidance, risk reduction, risk retention and risk transfer)
Risk Categories	Grouping of risks with similar characteristics used in establishing the clients risk portfolio.
Risk Profile	Identification and listing of risks, typically in order of highest to lowest based on a qualitative or quantitative measurement approved by client management.
Risk Strategy	The approach adopted for associating and managing risks based on the Department's objectives and strategies.
Risk Appetite	The amount of residual risk that the Institution is willing to accept.
Key performance indicators	These are quantitative measurements, both financial and non-financial, of the process's ability to meet its objectives and of the process' performance. They are usually analyzed through trend analyses within an entity or through benchmarking against a peer of the entity or its industry.

Probability	The likelihood that the risk will materialize.
Hazard	The source of or exposure to danger.
Incident	An undesired event as a result of a risk behavior, or high-risk conditions, without resulting in loss, but has the potential for losses.

1. INTRODUCTION

The purpose of this document is to outline an overall approach to risk management that addresses the risks facing Mpumalanga Department of Culture, Sport and Recreation in pursuing its strategy and which will facilitate the effective recognition and management of such risks.

The strategy is drawn up in order to ensure that risks are identified, appropriate remedial action is considered and where appropriate, a provision is made to implement risk reduction measures. Risk management is about managing threats and opportunities and, in so doing, creates an environment of "no surprises". This strategy will assist to embed the process of risk management within the governance structure of the department.

Risk management is both a statutory requirement and an indispensable element of good management. As such its implementation is crucial to the department and essential to its ability to discharge its various functions in accordance with its strategic plans.

Our risk management strategy provides a comprehensive framework and process designed to support members and officers in ensuring that the department is able to fully discharge its risk management responsibilities. The strategy outlines the objectives and benefits of managing risks, responsibilities for risk management, and provides an overview of the framework we will implement to manage risk.

Risk management in Mpumalanga Department of Culture, Sport and Recreation is about improving our ability to deliver our strategic objectives by managing our threats, enhancing our opportunities and creating an environment that adds value to ongoing service delivery activities.

Risk management is a central part of any organisation's strategic management. It is the process whereby an organisation 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 organisational management and is being promoted internationally and in South Africa as good business practice applicable to both the public and private sectors. This document sets out the Department's Enterprise-Wide Risk Management Strategy Framework.

Enterprise-Wide Risk Management (EWRM) is a structured, consistent and integrated approach that aligns strategy, processes, people, technology and knowledge to minimise risks to corporate goals and

maximise the achievement of objectives. Its purpose is to evaluate and manage the uncertainties the department faces to maximise opportunities. The Risk Management Framework supports risk management philosophy and practices, as embodied in the Risk Management Policy.

This document is applicable to all employees, contractors and business partners working for the department or any affiliated entity, program or initiative. The Risk Management Framework covers the full spectrum of risk taken in the pursuance of the department's strategic objectives: Strategic risks which originate from the possibility of a variance in the outcome of decisions and choices made in the setting of the department's strategic goals from what is expected to be achieved.

Operational risks arise from the possibility of a variance between the expected and actual performance, reliability, quality and efficiencies of the department's internal operations. The accounting authority has committed the department to a process of risk management that is aligned to the principle of good corporate governance, as supported by legislation and leading practice.

This strategy will be reviewed as and when there are key changes to the risk universe of the Department or guiding methodology.

LEGAL MANDATE

Since 1999 this practice has been further supported by the **Public Finance Management Act which stipulates in Section 38 that:**

"The accounting officer…has and maintains:

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

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, the internal audit units or the Audit Committee in this regard.

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.

The **King report on Corporate Governance**, 2016 also reflects on risk management as an integral part of strategic and operational activities.

The Public Sector Risk Management Framework defines Risk Management as "a systematic process to identify, evaluate and address risks on a continuous basis before such risks can impact negatively on the institution's service delivery capacity."

ISO 31000:2018, *Risk management – Guidelines*, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector.

2. OBJECTIVES OF THE STRATEGY

2.1 To develop a risk map which will identify and rank all significant risks facing the department and facilitate the achievement of the departmental strategy through proactive risk management.
2.2 To rank all risks in terms of the likelihood and occurrence and expected impact upon the department.
2.3 To allocate Clear roles, responsibilities and accountabilities for risk management.
2.4 To facilitate compliance with best practices in corporate governance.
2.5 To raise awareness of the principles and benefits of involved in the risk management process and to obtain staff commitment to the principles of risk control and,
2.6 To articulate processes applied to review the effectiveness of the systems of internal controls.

3. STRUCTURAL CONFIGURATION

Many institutions have difficulty in deciding the correct reporting lines for the risk management function. The main reason for this is that risk management embraces most aspects of the institution, such as strategy, finance, human resources, service delivery and public relations. In addition, the risk management function has close links to activities such as insurance, compliance, governance, internal audit and loss prevention. It is therefore understandable that the reporting lines for risk management are not immediately apparent.

In ideal circumstances the Chief Risk Officer (CRO) should report directly to the Accounting Officer given the latter's legal responsibility for risk management (Sec 38(1) (a) (i)) of the PFMA). However, where this is not practical because of the Accounting Officer large span of control and other operational factors, the Accounting Officer should delegate (Sec 44(1) (a) and (b)) to any person who is suitable and able to take up the responsibility.

On this basis, the accounting officer for the Department of Culture, Sport and Recreation (DCSR) has entrusted the Chief Risk Officer with the responsibility to ensure that the department has and maintains an effective, efficient and transparent systems of financial and risk management and internal control. Subsequently, the Chief Risk Officer will report functionally to the Risk Management Committee and administratively to the Accounting Officer. The Risk Management Committee should be involved in assessing the performance of the Chief Risk Officer.

The Risk Management Committee of the department is operational and is composed of General Managers, Senior Managers and Managers experts in their field of the department. The Department aims to enhance the work of the committee and to ensure that the committee is operating in line with best practices.

The department will appoint Risk Champions who will assist the Risk Management Unit to facilitate risk management activities in the department.

Risk Management Reports

The CRO is required to draft reports for the Executive Management and the Audit Committee. Management needs assurance that the risks have been identified and that their controls are working. The CRO then needs to receive risk and risk management information based on the requirements of King IV and other governance principles. On the other hand, the Audit Committee will tend to review the process of risk management, the control environment and losses related to risk. The CRO needs to then design an appropriate template for reporting to the Audit Committee.

Annual Report Statement

The CRO should draft the risk management statement for the annual report to stakeholders. Many institutions struggle with the issues of whether to disclose the specific contents of the risk registers. The institution's philosophy of stakeholder reporting and corporate governance should guide the decisions relating to risk reporting. The CRO should highlight the key risks areas of the institution, the involvement of Executive Management in risk management, the institutional arrangement for risk management, controls for risks and system of risk management.

4. RISK MANAGEMENT ACTIVITIES

In implementing the departmental risk management policy, we undertake the following:

To define and implement a context for risk management in the department by:

a) Developing a centrally co-ordinated risk framework and management process to ensure consistency throughout the department. This will include the development of a Fraud Prevention Plan.
b) Ensuring that risk management is not one event, but a series of continuous actions that permeate a department's activities.
c) Defining the responsibility structure for risk management throughout the department.
d) Developing a clear and unambiguous understanding of our strategic objectives and purpose.
e) Continually evaluating and reviewing the internal and external environment for risks that may affect the achievement of our strategic objectives.

f) Continually reviewing our risk tolerance as our internal and external environment changes.**To implement the following continuous risk management process in the department:**

a) An annual review of the most significant risks facing the organization.
b) Assessment and evaluation of the inherent impact and likelihood of risk occurring.
c) Determination of the department's response to the risk – (Take, Manage, Transfer (insure) or Avoid). Cost benefit as well as service delivery considerations will be a factor in deciding on the most suitable response.
d) Where the response is to manage or transfer the risk, we will examine existing procedures and controls in place to manage the risk to an acceptable level.
e) Re-evaluation of the risk after taking controls into account, to obtain the residual risk/ exposure.
f) Consideration of any enhancements to control that may be required to reduce residual exposure to an acceptable level.
g) Continual monitoring of the status of risks and developing a process for appropriate action if that status changes.
h) Reporting to senior management and the audit committee on an ongoing basis regarding the results and status of risk management throughout the department.
i) Maintaining an awareness of risk and risk management processes throughout the department.

5. ACCOUNTABILITY, ROLES AND RESPONSIBILITIES

5.1 Executive Authority

5.1.1 High level responsibilities of the Executive Authority in risk management include:

a) Providing oversight and direction to the Accounting Officer on the risk management related strategy and policies;
b) Having knowledge of the extent to which the Accounting Officer and management has established effective risk management in their respective departments;
c) Awareness of and concurring with the department's risk appetite and tolerance levels;
d) Reviewing the department's portfolio view of risks and considers it against the department's risk tolerance;
e) Influencing how strategy and objectives are established, departmental activities are structured, and risks are identified, assessed and acted upon;

f) Requiring that management should have an established set of values by which every employee should abide by;

g) Insist on the achievement of objectives, effective performance management and value for money.

5.1.2 In addition the Executive Authority should consider the following aspects below which if not considered could affect the department's risk culture:

a) The design and functioning of control activities, information and communication systems, and monitoring activities;

b) The quality and frequency of reporting;

c) The way the department is managed including the type of risks accepted;

d) The appropriateness of reporting lines.

5.2 Accounting Officer/ Head: Culture, Sport And Recreation

The Accounting Officer shall ensure that the responsibility for risk management vests at all levels of management and that it is not only limited to the Accounting Officer. The Accounting Officer shall also ensure that a risk assessment is conducted regularly to identify emerging risks.

High level responsibilities of the Accounting Officer include:

a) Setting the tone at the top by supporting enterprise risk management (ERM) and allocating resources towards the implementation thereof;

b) Establishing the necessary structures and reporting lines within the department to support ERM;

c) Approving the risk management strategy, risk management policy, risk management implementation plan and fraud risk management policy;

d) Approving the department's risk appetite and risk tolerance;

e) Influencing an departmental "risk aware" culture;

f) Approving the code of conduct for the department and holding management and officials accountable for adherence;

g) Place the key risks at the forefront of the management agenda and devote personal attention to overseeing their effective management;

h) Hold management accountable for designing, implementing, monitoring and integrating risk management principles into their day-to-day activities;

i) Holding the structures responsible for risk management activities accountable for adequate performance;

j) Ensuring that a conducive control environment exists to ensure that identified risks are proactively managed;

k) Leverage the Audit Committee, Internal Audit, Risk Management Committee and other appropriate structures for assurance on the effectiveness of risk management;

l) Provide all relevant stakeholders with the necessary assurance that key risks are properly identified, assessed, mitigated and monitored;

m) Consider and act on recommendations from the Audit Committee, Internal Audit, Risk Management Committee and other appropriate structures for improving the overall state of risk management;

n) Provide appropriate leadership and guidance to senior management and structures responsible for various aspects of risk management.

5.3 Management

In discharging their high level responsibilities relating to risk management, Management:

a) Acknowledges the "ownership" of risks within their functional areas and all responsibilities associated with managing such risks;

b) Cascades risk management into their functional responsibilities;

c) Empowers officials to perform adequately in terms of risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development;

d) Holds officials accountable for their specific risk management responsibilities;

e) Maintains the functional risk profile within the department's risk tolerance and appetite;

f) Provides reports on the functional risk management consistent with the department's reporting protocols (including appearing before committees);

g) Aligns the functional and departmental risk management methodologies and processes;

h) Implements the directives of the Accounting Officer concerning risk management;

i) Maintains a harmonious working relationship with the Chief Risk Officer and supports the Chief Risk Officer in matters concerning the functions risk management;

j) Maintains a harmonious working relationship with the Risk Champion and supports the Risk Champion in matters concerning the functions risk management;

k) Keeps key functional risks at the forefront of the management agenda and devote personal attention in overseeing the management of these risks.

5.4 Chief Risk Officer

High level responsibilities to achieve this include:

a) Working with senior management to develop the overall enterprise risk management vision, risk management strategy, risk management policy, as well as risk appetite and tolerance levels for approval by the Accounting Officer;

b) Communicating the risk management policy, risk management strategy and risk management implementation plan to all stakeholders in the department;

c) Setting up of the risk management structure and risk management reporting lines within the department;
d) Continuously driving the risk management process towards best practice;
e) Developing a common risk assessment methodology that is aligned with the department's objectives at strategic, tactical and operational levels for approval by the Accounting Officer.
f) Coordinating risk assessments within the department / branches / division / unit on a regular basis.
g) Sensitising management timeously of the need to perform risk assessments for all major changes, capital expenditure, projects, departmental restructuring and similar events, and assist to ensure that the attendant processes, particularly reporting, are completed efficiently and timeously.
h) Assisting management in developing and implementing risk responses for each identified material risk;
i) Participating in the development of the combined assurance plan for the department, together with internal audit and management;
j) Ensuring effective information systems exist to facilitate overall risk management improvement within the department;
k) Continuously transferring risk management principles and practices, through training interventions, to all stakeholders within the department;
l) Advising management in the development of financing structures;
m) Performing a PEST(EL) analysis to identify emerging risks facing the department for further action and intervention;
n) Collating and consolidating the results of the various assessments within the department;
o) Analysing the results of the assessment process to identify trends, within the risk and control profile, and develop the necessary high level control interventions to manage these trends;
p) Compiling the necessary reports to the Risk Management Committee;
q) Providing input into the development and subsequent review of the fraud prevention strategy, business continuity plans, occupational health, safety and environmental policies and practices and disaster management plans.

5.5 Risk Management Committee

In discharging its oversight responsibilities relating to risk management, the Risk Management Committee has the following high level responsibilities:

a) Review the risk management policy and strategy and recommend for approval by the Accounting Officer;
b) Review the risk appetite and tolerance and recommend for approval by the Accounting Officer;

c) Review the department's risk identification and assessment methodologies to obtain reasonable assurance of the completeness and accuracy of the risk register;
d) Evaluate the effectiveness of mitigating strategies to address the material risks of the Department;
e) Report to the Accounting Officer any material changes to the risk profile of the Department;
f) Review the fraud prevention policy and recommend for approval by the Accounting Officer;
g) Evaluate the effectiveness of the implementation of the fraud prevention policy;
h) Review any material findings and recommendations by assurance providers on the system of risk management and monitor that appropriate action is instituted to address the identified weaknesses;
i) Develop goals, objectives and key performance indicators for the Committee for approval by the Accounting Officer;
j) Develop goals, objectives and key performance indicators to measure the effectiveness of the risk management activity;
k) Set out the nature, role, responsibility and authority of the risk management function within the Department for approval by the Accounting Officer, and oversee the performance of the risk management function;
l) Provide proper and timely reports to the Accounting Officer on the state of risk management, together with aspects requiring improvement accompanied by the Committee's recommendations to address such issues.

5.6 Audit Committee.

In discharging its oversight responsibilities relating to risk management, the audit committee:

a) Gains thorough understanding of the risk management policy, risk management strategy, risk management implementation plan, and fraud risk management policy of the department to enable them to add value to the risk management process when making recommendations to improve the process;
b) Reviews and critiques the risk appetite and risk tolerance, and recommends this for approval by the Accounting Officer;
c) Reviews the completeness of the risk assessment process implemented by management to ensure that all possible categories of risks, both internal and external to the department, have been identified during the risk assessment process. This includes an awareness of emerging risks pertaining to the department.
d) Reviews the risk profile and management action plans to address the risks;
e) Reviews the adequacy of adapted risk responses;
f) The audit committee must monitor the progress made with the management action plan;

g) Reviews the progress made with regards to the implementation of the risk management strategy of the department;
h) Facilitates and monitors the coordination of all assurance
i) activities implemented by the department;
j) Reviews and recommends any risk disclosures in the annual financial statements;
k) Provides regular feedback to the Accounting Officer on the effectiveness of the risk management process implemented by the department;
l) Review the process implemented by Management in respect of fraud prevention and ensure that all fraud related incidents have been followed up appropriately;
m) Reviews and ensures that the internal audit plans are aligned to the risk profile of the department;
n) Review the effectiveness of the internal audit assurance activities and recommends appropriate action to address any shortcomings.

ERM architecture and high level responsibilities of Internal Audit

Although, best practice indicates that Internal Audit should not be in direct control of the risk management function, Internal Audit may perform advisory and consulting engagements on risk management in accordance with applicable standards (refer to the International standards for the Professional Practice of Internal Auditing - Performance standard 2110).

Responsibilities of Internal Audit in risk management include:

- Reviewing the risk philosophy of the institution. This includes the risk management policy, risk management strategy, fraud prevention plan, risk management reporting lines, the values that have been developed for the institution;
- Reviewing the appropriateness of the risk tolerance levels set by the institution taking into consideration the risk profile of the institution;
- Providing assurance over the design and functioning of the control environment, information and communication systems and the monitoring systems;
- Providing assurance over the institution's risk identification and assessment processes;
- Utilizing the results of the risk assessment to develop long term and current year internal audit plans;
- Providing independent assurance as to whether the risk management strategy, risk management implementation plan and fraud prevention plan have been effectively implemented within the institution;Providing independent assurance over the adequacy of the control

environment. This includes providing assurance over the effectiveness of the internal controls implemented to mitigate the identified risks.

➢ **Responsibilities of Other Personnel in Risk Management**

Other Personnel is defined as:

- Employees within the institution with non-specific risk management responsibilities;
- All employees of the Institution including general staff, stakeholders and contractors with non-specific risk management responsibilities

Other Personnel are responsible to ensure that the risk management process has been integrated into the day-to-day activities of the institution.

High level responsibilities include:

- Familiarity with the overall enterprise risk management vision, risk management strategy, fraud risk management policy and risk management policy;
- Acting in terms of the spirit and letter of the above;
- Applying the risk management process to their respective roles;
- Focusing upon identifying risks and reporting these to the relevant risk owner. Where possible and appropriate, manage these risks;
- Acting within the risk appetite and tolerance levels set by the business unit;
- Adhering to the code of conduct for the institution;
- Maintaining the functioning of the control environment, information and communication as well as the monitoring systems within their delegated responsibility;
- Providing information and cooperation with other role players;
- Participation in risk identification and risk assessment within their business unit.

ELEMENTS

All risks facing the department whether quantified or not are to be considered. Several types of risk that are not easily quantified can potentially hold significant impact on the department, e.g. reputational risks.

All risks facing the department will be evaluated based on the likelihood of the risk occurring as well as the impact on the department if the risk event were to occur. The likelihood and impact of each risk is evaluated both at an inherent (without management) and residual (with management) level.

The following elements are essential when managing risk:

- ✓ **Assurance:** Stakeholders are assured that risks are being managed within The department's risk tolerance and receive information regarding the quality and type of control in place.
- ✓ **Oversight and responsibility:** All critical risks facing the department have been identified, managed at a level and frequency that support the department's risk tolerance.

- ✓ **Ownership:** Risk owners are assigned and understand their responsibility for management, oversight and assurance.

Risk response for identified risks will be assessed according to the department's risk appetite. The five possible risk responses are to:

- ✓ Avoid (eliminate) the risk
- ✓ Reduce (mitigate) the risk
- ✓ Transfer the risk (e.g. insurance);
- ✓ Share the risk; or
- ✓ Accept the risk.

There will be a desire to learn from events that have transpired – the risk management process is a cycle where experience provides key information for new decisions and actions. Open and appropriate communication of results and lessons learned is required to facilitate learning.

The department's risk register will be evaluated annually. New risks will be considered. Risks no longer relevant will be removed. The risk register will be refreshed by rating the likelihood and impact for each risk. This information is used to prioritize the risks and this in turn flows into the department.

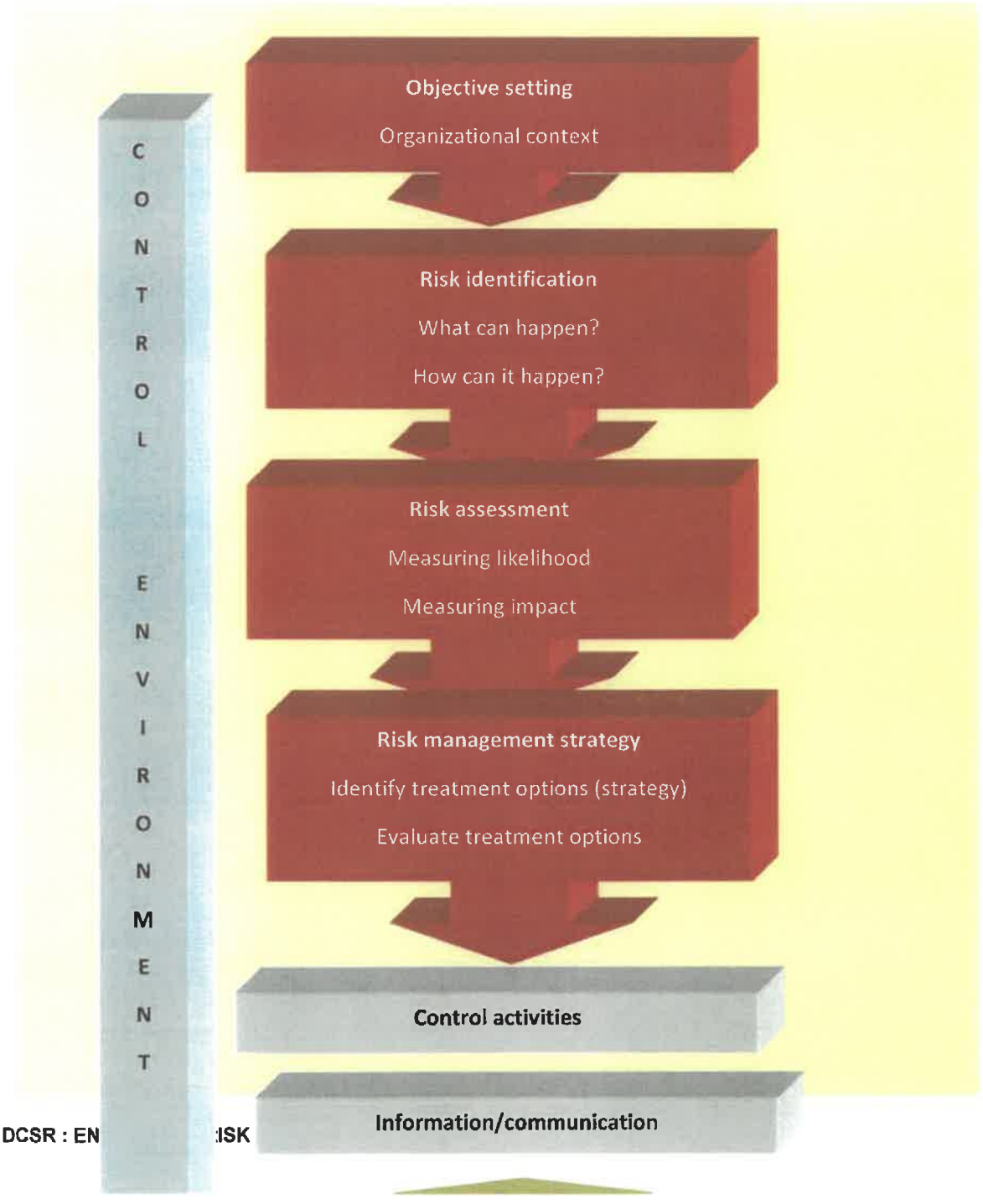
LIMITATION OF DEPARTMENTAL RISK MANAGEMENT

Effective risk management, no matter how well designed and operation, provides only reasonable assurance to management regarding achievement of the department's objectives. Achievement of objective is affected by limitations inherent in all management processes. These include the realities that human judgement in decision-making can be faulty and that breakdown can occur because of such human failures as simple error of mistake. Additionally controls can be circumvented by collusion of two or more people, and management has the ability to override the enterprise risk management process, including risk response decisions and control activities. Another limiting factor is the need to consider the relative costs and benefits of risk response.

RISK MANAGEMENT COMPONENTS

The process of managing risk is a structured approach for incorporating risk management into the daily, broader management process. Risk management is more than an exercise of risk avoidance. It is as much about identifying opportunities as avoiding or mitigating losses.

The following table indicates the different relationships between the components:



COMPONENT 1: CONTROL ENVIRONMENT

The department's 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 control environment consists of ten different layers that should all be present and functioning. The ten layers are discussed below:

a. Risk management philosophy

Management recognises that its philosophy and operating style affects the way the department is managed, including the kinds of risks accepted. The department relies more on written policies, standards of behavior, performance indicators and exception reports.

b. Risk tolerance

Risk appetite is the amount of risk that the department is willing to accept in pursuit of value. Management has identified some risks and established the tolerance level in respect of the risks that have been identified

c. Risk culture

Risk culture is the set of shared attitudes, values and practices that characterize how the department considers risks in its day-to-day activities. Employees are encouraged to consider the impact of potential events on other directorates and on the department as a whole.
To promote an effective risk culture the Department ensures that newly appointed employees are inducted to better understand its risk context and philosophy.

d. Executive authority

The executive authority is a critical part of the control environment and significantly influences other control environment elements. Their independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and appropriateness of its actions all play a role. Factors include the degree to which difficult questions are raised and pursued with management regarding strategy, plans and performance, and interaction that the audit committee has with internal and external auditors.

e. Integrity and values

The Department is guided by the following core values:

- All services rendered must be of par excellence
- All services must be rendered in a manner which is equitable, efficient, effective, accessible and of satisfactory quality
- All services must be in line with the 'Batho Pele' principles
- Commitment to high performance and continuous improvement of the capacity of its personnel
- Open communication, transparency and consultation.
- Personnel must adhere to the Code of Conduct
- Personnel must adhere to all legislations.

f. Commitment to competence

Management specifies the competency levels for particular jobs and translates those levels into requisite knowledge and skills. Job descriptions are developed for all positions that the department has established. Such job descriptions enable the Department to ensure that the duties of the employees are in line with the strategic goals and mandate of the Department.

g. Philosophy and operating style

Management's philosophy and operating style affect the way the department is managed, including the kinds of risks accepted. A department that has been successful accepting significant risks may have a different outlook on risk management than one that has faced harsh economic or regulatory consequences as a result of venturing into dangerous territory.

h. Authority and responsibility

The department will ensure that all delegations of authority are signed and adhered to.

i. HR policies and procedures

Human resource policies and practices pertaining to hiring, orientation, training, evaluating, counseling, promoting, compensating and taking remedial actions send massages to employees regarding the expected levels of integrity, ethical behavior and competence.

All senior managers include Risk Management as a key performance indicator with a weight in their performance agreements.

COMPONENT 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". Target and goal setting must be supported by thorough research and data analysis. The risks and opportunities should be identified prior to adoption of Annual Performance Plans.

Department Objectives can be viewed in the context of 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. Where the safeguarding concept applies to the prevention or timely detection of unauthorised acquisition, use or disposition of departmental assets.

COMPONENT 3: RISK IDENTIFICATION

Risk identification is the systematic identification of risk events arising as a result of inadequate or failed internal processes, people and systems or external events (i.e. what can go wrong) potentially resulting in strategic and business objectives not being achieved. The identification also includes the cause as well as the consequence (effect) of the risk event.

Events with a potentially negative impact represent risks, which require management's assessment and response.

A risk event is described as an event, which could result in the organization not achieving its strategic and business objectives.

The risk event must be a cause as well as the potential consequence (effect) in order to give a clearer understanding of the risk. This may be illustrated by a simple example:

Risk- a virus enters the computer server

Cause -inadequate virus protection software

Effect-loss of data and software failure with potential loss and reputation damage.

The process of risk identification requires careful consideration of corporate level strategic objectives, business unit level strategic objectives; business processes and external environment in which the department operates to identify events of circumstances that can arise that would prevent the department from achieving its objectives or result in ineffective and inefficient processes.

Each objective or process is considered individually with the risk categories and risk prompts being used to identify risk events. Risk categories are included as Annexure A and risk prompts are included as Annexure A. The risk prompts are not exclusive and are intended to serve as assistance in identifying risk.

It is important to understand that in identifying risk, at this stage in the process, no consideration is given to the likelihood of the risk event occurring nor to the quantum of the impact should the risk event materialize. These activities take place in the risk assessment process.

The initial risk identification will be undertaken through a workshop facilitated by risk specialists. However, risk identification is a dynamic and ongoing process and the Chief Risk Officer and the individual core function managers will need to review and update the risk register on an ongoing g basis.

The following are Possible Methods of Identifying Risks

- Interview/ focus group discussion
- Audits or physical inspection
- Brainstorming
- Survey, questionnaire, Delphi technique
- Examination of personal experience or department experience
- Scenario analysis, operational modeling, flow charting, threats (SWOT) analysis
- Incident, accident, injury investigations and databank of risk events which have occurred.

Possible sources of Risk

- new activities and services
- disposal or cessation of current activities
- outsourcing to external service providers
- commercial/ legal changes
- personnel/ human behavior
- behavior of contractors/ private suppliers
- financial market conditions
- occupational health safety, natural events and misinformation

The output of the risk identification will be an initial risk register, which lists all the identified risks and will be used throughout the balance of the risk management process.

Retrospective / Prospective / Categorization

Retrospective

When identifying risk the retrospective approach could be used, which means that past events (risks) that have occurred are evaluated. One of the sources of such information would be the incidents and/or accidents register, audit reports, newspapers and/or professional media and customers complaints.

Prospective

When exploring the prospective approach it means that events (risks) that could potentially happen are evaluated, that also include but is not limited to events (risks) that are currently being managed. Some of the other sources of such information would be the SWOT analysis, brainstorming with staff members and or external stakeholders, interviews with staff members, a survey in the form of questionnaire and process flow charting or system description.

Categorisation

When exploring the categorisation approach it means events that could fall within the predetermined categories are evaluated, for the purposes of this methodology, the following categories refer:

- Strategic – relating to high level goals, aligned with and supporting the department's mission/vision
- Operations – relating to the effectiveness and efficiency of the department's operations, including performance and service delivery goals
- Reporting – relating to the effectiveness of the department's reporting (internal and external reporting) that may involve financial and/or non-financial information
- Compliance – relating to the department's compliance with applicable laws and regulations
- Safeguarding – relating to prevention of loss of a department's assets or resources, whether through theft, waste or inefficiency. Where safeguarding concept applies to the prevention or timely detection of unauthorized acquisition, use, or disposal of the department's assets.

When capturing risks the bigger picture must be kept in mind - the risk is the possibility of something happening with the potential to undermine the achievement of objectives in the most effective, efficient and economic manner. The risk should therefore contain the threat and consequence to ensure the essence of the risk is captured rather than just capturing the threat or the consequence only.

The business risk identification process will take the following into consideration:

- A situational analysis inclusive of an assessment of both external and internal environmental factors was performed.

- The identification and rating of business risks that have the potential to impact (positively or negatively) on the achievement of Department's strategic objectives.
- Reports from Internal Audit, Auditor General South Africa and Oversight committees i.e. SCOPA and Portfolio Committees reports were used as a basis for the risk assessment process.
- Management should identify the risk appetite and tolerance levels for each strategic risk.
- A valuable tool and reference source for management, assisting management in identifying and/or managing strategic risks including financial, operational, compliance and reputational risks.
- The initial business risk profile will form the basis of an ongoing review and re-rating process of risks at Department. The determination of the proposed focus of the detailed risk management approach (i.e. risk management implementation plan).
- The development and rollout of mapped controls and an action plan process at Department.
- Should the Department opt to use the Delphi technique as an additional technique to discuss the risks, this will either be done in a structured one-on-one basis or a workshop. Participants to the risk assessment workshop will be comprised of executive, senior and middle management for strategic risk identification purposes and assistant managers to more operational staff for all operational risks including Information Communication Technology, fraud, Occupational Health and Safety to name a few.

The risk categories have been aligned with strategic objectives in order to identify those risks that directly affect and/or impede your ability to achieve your strategic and business objectives. Such business objectives were directly extracted from the five year and annual performance plan.

Limitations

If risks are improperly assessed and prioritised, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur. Qualitative risk assessment is subjective and lacks consistency. The primary justification for a formal risk assessment process is legal and bureaucratic.

Prioritising the *risk management processes* too highly could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete

COMPONENT 4: RISK ASSESSMENT

- ✓ Risk assessment is a method of analysing and documenting the consequence (impact) and likelihood (probability) of the identified risk events occurring that will prevent the achievement of business objectives.
- ✓ The initial risk assessment (inherent risk) is the scoring of the consequence (impact and likelihood of potential events that could occur in NO controls were in place (i.e. the effect if all controls failed.
- ✓ The likelihood (probability) of the risk event is established using the following rating scale:

The impact of the risk is then assessed assuming that the risk will occur, ignoring the likelihood or considering the likelihood as certain.

There are numerous methods of assessing impact ranging from basic to sophisticated and from highly subjective to objective quantification. The more sophisticated and objective the impact assessment, the more effort is required.

For the initial risk assessment, a basic subjective approach will be adopted based on the following rating scale:

RATING	ASSESSMENT	DEFINITION
1	Insignificant	Negative outcomes or missed opportunities that are likely to have a negligible impact on the ability to meet objectives
2	Minor	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives
3	Moderate	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives
4	Major	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives
5	Critical	Negative outcomes or missed opportunities that are of critical importance to the achievement of the objectives

Once the initial risk process is complete, the highest rated risks will be subjected to more sophisticated and quantifiable impact assessments. The methods for doing these assessments will be decided upon by the risk committee.

The risk register will be updated with the likelihood and impact assessment for each risk and the inherent risk rating will be calculated.

The specific fields in the risk register that will be competed are:

NAME	DESCRIPTION
Likelihood	The probability that the risk event will materialize
Impact	Impact on the business should the risk event materialize
Inherent Risk Rating	The combination of the likelihood and impact of the risk

RISK EVALUATION

- Bearing in mind, that the inherent risk rating assumes that there are no controls in place, it is necessary to evaluate the risk taking into account the existing controls that may mitigate either the impact or likelihood of the risk event materialising.
- Controls are any methods, procedures, equipment or other actions implemented by management (either consciously or unconsciously) that may mitigate, either
  - ✓ The likelihood or impact, of a particular risk event and provide additional assurance that objectives will be achieved.
  - ✓ Each risk may require one or multiple controls in order to effectively reduce the risk/threat to a level, which is acceptable to management and other stakeholders
- The controls documented and used for the risk evaluation are the *current controls* in place. Planned amendments to existing controls or new controls are documented and assessed as part of risk planning.
- Each risk is considered in terms of the existence of any current controls in place that may mitigate the risk. The controls must be identified and described.

An assessment of the effectiveness of the current controls must be performed based on the following scale:

RATING	ASSESSMENT	DEFINITION	PERCENTAGES
1	No control	There are no controls in place	0%
2	Not effective	There are limited controls in place with major deficiencies	1-20%
3	Control needs improvement	There are controls in place but they are either not effective or not being adhered to.	21-40%
4	Controls are adequate	There are controls in place but require improvement to make them effective.	41-60%
5	Effective	There are controls in place which are implemented and effective.	61-80%
6	Highly effective	There are controls in place which are implemented and highly effective	81-90%

- The risk register will be updated with the control description and control effectiveness rating, which will allow the calculation of an initial residual risk rating.
- The downward adjustment of the inherent risk will be performed in terms of the inherent risk adjustment .This will not be a formulaic adjustment, but will require due consideration by those assessing and evaluating risk. The result is the residual risk rating based on the current control environment, which will be utilised for risk response planning.
- The risks will be prioritised according to this rating, which will be used for risk planning.

The specific field in the risk register that will be completed are:

FIELD	NAME	DESCRIPTION
1	Current Control	This is a brief description of the controls currently in place that may mitigate the probability and impact of the risk event
2	Current Control Effectiveness	This is an effectiveness assessment based on the effectiveness of the current controls in place in mitigating risk
3	Residual Risk	This is the downward adjusted inherent risk likelihood based on the controls

Example: Certainty of occurrence		
Score	**Likelihood**	**Occurrence**
5	Common	The risk is already occurring, or is likely to occur more than once within the next 12 months.
4	Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months.
3	Moderate	There's an above average chance that the risk will occur at least once in the next 3 years.
2	Unlikely	The risk occurs in frequently and is likely to occur within the next 3 years.
1	Rare	The risk is conceivable but only likely to occur in extreme circumstances.

RISK PLANNING

- The prioritized list of risk events needs to be examined by the department to determine how to respond to the various identified risks.
- This is a management responsibility requires a careful review of each risk, taking into consideration the departments risk appetite and associated costs and benefits, to arrive at a set of appropriate risk response strategies.
- There are fundamentally four risk response strategies as follows:

There are four ways in which risks could be managed or treated:

- Risk Avoidance/Terminate
- Risk Control/Treat
- Risk Transfer/Sharing
- Risk Retention/Tolerate

The various risk treatment approaches can be summarized as follows:

Risk Treatment Approach	Brief Description
Risk Avoidance/Terminate	One method of dealing with risk is to avoid the risk by not proceeding with the activity likely to generate the risk. Risk avoidance should only occur when control measures do not exist or do not reduce the risk to an acceptable level. Inappropriate risk avoidance may result in missed opportunities and increase in the significance of other risks.
Risk Transfer/Sharing	Part or most of a risk may be transferred to another party so that responsibility is shared. Mechanisms for risk transfer include contracts, insurance, partnerships and business alliances. It is important to note that risks can never be completely transferred, because there is always the possibility of failures that may impact on the institution. Transfer of risk may reduce the risk to the original institution without changing the overall level of risk.
Risk Control/Treat	Risk control involves identifying options for treating or controlling risk, in order to either reduce or eliminate negative consequences, or to reduce the likelihood of an adverse occurrence. Risk control should also aim to enhance positive outcomes.

	Controls should not be: - Control < Risk Controls not effective - Control > Risk Controls not economic - Control = Risk Controls are efficient
Risk Retention/ Tolerate	Low or tolerable risks may be accepted. Acceptance means the institution chooses to accept that the risk exists, either because the risk is at a low level or the cost of treating the risk will outweigh the benefit. Risk retention does not mean that nothing is done in order to deal with the risk, but rather that at the present time the decision is to deal with the risk by way of routine procedures that already exist – re-focusing attention on the risk and re-emphasizing the importance of existing policies and procedures.

There always exists a trade-off between the level of risk and the cost of reducing a risk to an acceptable level – the cost of treating a risk must be commensurate with the benefits likely to be obtained. In finalizing risk treatment approaches, a cost-benefit analysis must be performed. This can be quite complex, especially if one considers that the costs and benefits are not necessarily quantifiable. Both quantitative and qualitative costs and benefits must be considered. Furthermore, the cost of implementing a specific treatment approach must be weighed against the potential loss if the particular approach is not implemented.

- Risk action plan that may be required to either improve an existing control, or implement a new control to reduce the assessed risk need to be developed for each risk, primarily where a reduction of risk is selected as the risk response strategy.
- Once the risk response category has been identified for particular risk, specific actions must then be devised to reflect that response. Commonly it is not possible to remove a risk in it's entirely (unless a different business activity is adopted altogether). Hence where a risk can be reduced to within acceptable limits and the cost of the risk response actions do not outweigh the benefits, it is possible to retain a risk while carrying out reduction strategies.
- The consideration of risk management strategies and the action plan is integral to risk management and requires that management select a response that is expected to bring risk likelihood and impact within the organization's risk tolerance level.
- Management should recognize that some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainly and limitations inherent in all activities.

- Specific care must be exercised for risks that are regarded as low probability but high impact (referred to as "black swan"), including the recognition that the probability of occurrence of occurrence of an unpredictable sever event is much greater than is generally recognized. The most effective way to mitigate such risks may ultimately be by way of business continuity plans, including consideration of capital adequacy as the ultimate mitigating factor. Management should consider such exposures and mitigating actions as part of their annual assessment of the going concern assumption.
- The risk register must be updated to reflect additional planned controls and actions to reduce the risk. The likelihood and impact rating need to be reassessed taking into account the risk strategy adopted and additional planned controls and actions to reduce the risk, which may result in a downward adjusted residual risk profile.

The specific fields in the risk register that will be completed are:

Field	Name	Description
1	Action Plan	This is a brief description of the controls/actions that are planned to mitigate the probability and impact of the risk event.
2	Action Owner	Allocation of certain tasks to employees.
3	Risk Owner	This is the Programme manager who will ensure that the action plan is implemented.
4	Due Date	This is the date by which the action plan will be implemented.

The risk strategy provides guidance on how to reduce the organizations risk vulnerability inherent in its business and operational strategies to levels acceptable within its risk appetite.

The risk strategy is informed by the risk appetite and defines which risks should be avoided and which should be accepted and retained or accepted but modified by way of mitigation, transfer or sharing of risk.

Where the business and operational strategies put upward pressure on the risk exposure, the risk strategy exerts a downward influence on the inherent risk exposure by giving guidance on the best options for minimizing uncertainty and actions for maintaining residual risk exposure at tolerable levels.

Budget Consideration: the required funding will need to be secured for the success of the implementation.

Overall, successful implementation requires effective management within the total management process consisting of planning, organizing, directing and monitoring. Specific issues that need to be addressed in the risk management strategy should include:

- Obtaining approval for the initial implementation plan at all appropriate levels.
- Clear assignment of responsibilities to risk owners. Responsibilities should be borne by those individuals who are directly involved with the risk, and they must take responsibility for the specific function or activity affected by a particular risk treatment measure and who are in the best position to control and supervise the risk (risk owners).
- Drawing up detail specifications for the treatment plan (user, control and technical specifications, due dates), as appropriate. Specifications also include defining the expectations of the specific treatment plans (the treatment standards), i.e. what results can we expect once the treatment measures concerned have been implemented successfully and the due date for the implementation of the treatment plan has been met
- Allocation of certain tasks to employees. This includes requirements for reporting on specific tasks.
- Consideration of the budget allocation. The required funding will need to be secured.
- Prepare facilities and personnel for implementation and integration into the existing organization, taking cognizance of existing policies, processes and procedures.
- Integration must be properly controlled, supervised and reported on in accordance with the allocation of tasks to individuals and the assignment of specific responsibilities
- Post-implementation review to ensure that all specifications have been met and that an effective implementation process has been carried out.

Every implementation process will be unique and must be managed accordingly. Implementation is influenced by the surrounding circumstances of the implementation, the nature of the risk treatment measures to be implemented and the policies, processes and procedures affected.

The risk strategy is illustrated in the table below:

RISK INDEX	RISK MAGNITUDE	RISK APETTITE	PROPOSED ACTIONS
20 – 25	Maximum risk	Unacceptable	Take immediate action to reduce risk with higher priority – Accounting Officer attention.
15 – 19	High risk	Unacceptable	
10 – 14	Medium risk	Acceptable	Take immediate action to reduce risk with high priority – Management attention.
5 – 9	Low risk	Acceptable	No risk reduction – control, monitor, inform management.
1 – 4	Minimum risk	Acceptable	No risk reduction – control, monitor, inform management.

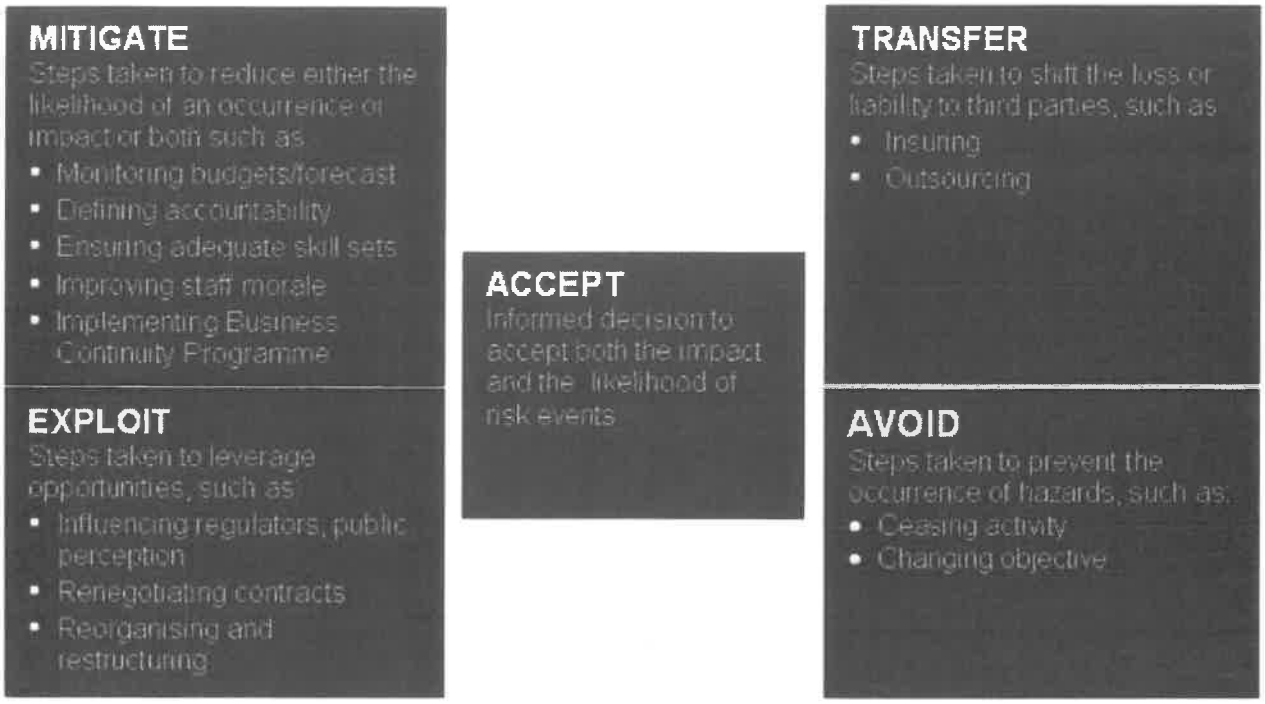
Management identifies risk management strategy options, which should include a fraud prevention plan and consider their effect on event likelihood and impact, in relation to risk tolerances, costs versus benefits, and thereafter designs and implements response options.

Risk Management strategies fall within the categories of risk avoidance, reduction, sharing and acceptance.

The risk response plan usually provides detail on:

- actions to be taken and the risks they address;
- who has responsibility for implementing the plan;
- what resources are to be utilized;
- the budget allocation;
- the timetable for implementation;
- details of the mechanism and frequency of review of the status of the response plan.
- Risk response options are not necessarily mutually exclusive or appropriate in all circumstances.

See diagram below:



- **ii) Select options for response**
- Once risks have been assessed and a level of risk rating has been assigned, an option for response is selected.

  There are four potential scenario's that could lead to different response options: See example below:

Scenario's	Response Option
a) High likelihood and High Consequence	Avoid/Mitigate
b) High Likelihood and Low Consequence	Exploit/Mitigate
c) Low Likelihood and High Consequence	Transfer (e.g. Insurance)
d) Low Likelihood and Low Consequence	Accept

Risk categories

As the risk environment is so varied and complex it is useful to group potential events into risk categories. By aggregating events horizontally across an institution and vertically within operational units, management develops an understanding of the interrelationship between events, gaining enhanced information as a basis for risk assessment.

The main categories to group individual risk exposures are as follows:

Risk type	Risk category	Description
Internal	Human resources	Risks that relate to human resources of an institution. These risks can have an effect on an institution's human capital with regard to: • Integrity and honesty; • Recruitment; • Skills and competence; • Employee wellness; • Employee relations; • Retention; and • Occupational health and safety.
	Knowledge and Information management	Risks relating to an institution's management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: • Availability of information; • Stability of the information; • Integrity of information data; • Relevance of the information; • Retention; and • Safeguarding.
	Litigation	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: • Claims by employees, the public, service providers and other third party • Failure by an institution to exercise certain right that are to its advantage
	Loss \ theft of assets	Risks that an institution might suffer losses due to either theft or loss of an asset of the institution.

	Material resources (procurement risk)	Risks relating to an institution's material resources. Possible aspects to consider include: • Availability of material; • Costs and means of acquiring \ procuring resources; and • The wastage of material resources
	Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the citizens.
	Information Technology	The risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: • Security concerns; • Technology availability (uptime); • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology.
	Third party performance	Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non-performance could include: • Outright failure to perform; • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
	Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the institution.

	Disaster recovery / business continuity	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: • Disaster management procedures; and • Contingency planning.
	Compliance \ Regulatory	Risks related to the compliance requirements that an institution has to meet. Aspects to consider in this regard are: • Failure to monitor or enforce compliance • Monitoring and enforcement mechanisms; • Consequences of non-compliance; and • Fines and penalties paid.
	Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
	Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: • Cash flow adequacy and management thereof; • Financial losses; • Wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and • Increasing operational expenditure.
	Cultural	Risks relating to an institution's overall culture and control environment. The various factors related to organizational culture include: • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values;

		• Goal alignment; and • Management style.
	Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
External	Risk category	Description
	Economic Environment	Risks related to the institution's economic environment. Factors to consider include: • Inflation; • Foreign exchange fluctuations; and • Interest rates.
	Political environment	Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include: • Political unrest; • Local, Provincial and National elections; and • Changes in office bearers.
	Social environment	Risks related to the institution's social environment. Possible factors to consider include: • Unemployment; and • Migration of workers.
	Natural environment	Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as: • Depletion of natural resources; • Environmental degradation; • Spillage; and • Pollution.
	Technological environment	Risks emanating from the effects of advancements and changes in technology.

	Legislative environment	Risks related to the institution's legislative environment e.g. changes in legislation, conflicting legislation.

COMPONENT 6: CONTROL ACTIVITIES

Section 38 (1) (a) of the PFMA, 1999 requires that the accounting officer must ensure that the department has and maintains—*(i) effective, efficient and transparent systems of financial and risk management and internal control;*

For any control to be effective, controls must be adequate. Internal controls are designed to reduce risks. Risks are the probability that losses may occur. If the controls are adequate the probability of loss reduces.

Internal auditors have the responsibility to assess the adequacy of internal control and must provide assurance that the controls will effectively reduce the risk of achieving objectives.

Broad internal control focus areas:

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

- Custody and accountability for resources
- Prompt and proper recording and classification of transactions
- Authorization and execution of transactions
- Documentation
- Management supervision and review Computer controls
- Access controls
- Adequate segregation of duties

- **Application Controls**

Completeness Controls

Controls should exist for all important data fields. Thus it is necessary to establish which data needs to be controlled. Completeness controls for input of data should ensure that all transactions are recorded, input and accepted and that each transaction is processed only once (i.e. duplicate transactions prevented).

Completeness controls for update of data should ensure that all transactions input and accepted are updated to a master file.

Completeness controls should include controls to ensure rejected transactions are resubmitted.

Completeness controls are concerned only with the recording of the transaction, not with the accuracy of the transaction data.

- **Accuracy Controls**

Accuracy controls for input of data should ensure that the initial recording of data from source to input documents is accurate and that conversion of data to machine readable form takes place accurately.

Accuracy controls for update of data should ensure that data is accurately carried through intermediate processing and accurately updated to the master file.

As for completeness controls, accuracy controls should include controls to ensure rejected data is corrected and resubmitted. Examples of accuracy controls are set out in Appendix 1 and explained in the following sections.

- **Validity Controls**

Validity controls should ensure that only valid (authorised) data is written to master files or printed on reports. Data is usually authorised at input stage, but output may be authorised.

Validity controls should include controls to ensure that unauthorised data is rejected.

- **Maintenance Controls**

Maintenance controls should ensure that data stored on file cannot be changed other than by normal controlled processing (correctness of data), that data is kept current and unusual data requiring action identified (currency of data).

Maintenance controls should also ensure that the correct generation of master file is used in updating (correctness and currency).

The auditor may also need to consider controls over the completeness, accuracy and validity of amendments, particularly if amendments are computer generated. These controls will be of the same nature as controls over transaction data.

In a new system, controls over file creation are also important. All data on a new file should be checked for completeness, accuracy and validity, before transactions are processed against it.

In evaluating controls over amendments to files and file creation general controls will need to be considered.

COMPONENT 7: INFORMATION AND COMMUNICATION

Pertinent 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 is needed at all levels of the department to identify, assess and respond to risks, and to otherwise run the department and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Information comes from many sources internal and external, and in quantitative and qualitative forms and allows risk management responses to changing conditions in real time.

The challenge for management is to process and refine large volumes of data into relevant and actionable information. This challenge is met by establishing an information systems infrastructure to source, capture, process, analyse and report relevant information. These information systems – usually computerized but also involving manual inputs or interfaces – often are viewed in the context of processing internally generated data relating to transactions.

Information systems have long been designed and used to support department strategy. This role becomes critical as departments need change and technology creates new opportunities for strategic advantage. To support effective risk management, a department captures and uses historical and current data. Historical data allow the department to track actual performance against targets, plans and expectations. It provides insights into how the department performed under varying conditions, allowing management to identify correlations and trends and to forecast future performance. Historical data also can provide early warnings of potential events that warrant management attention.

Present or current state data allow a department to assess its risks at a specific point in time and remain within established risk tolerances. Current state data allow management to take a real-time view of existing risks inherent in a process, function or unit and to identify variations from expectations. This provides a view of the department's risk profile, enabling management to alter activities as necessary to fit in with the acceptable level of risk

Information is a basis for communication, which must meet the expectations of groups and individuals, enabling them to effectively carry out their responsibilities. Among the most critical communications channels is that between top management and the executive authority.

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.

Management provides specific and directed communication addressing behavioural expectations and the responsibilities of personnel. This includes a clear statement of the department's risk management philosophy and approach and delegation of authority.

Information must be fed into the organization in the form of a series of triggers and reports. These includes, inter alia:

Name	Description	Frequency
Top 10 risks	The top 10 risks with the highest residual risk rating	Monthly
Risk register	The register of all identified risks within the department	Quarterly
Incident report	Actual non-compliance incidences and losses incurred	As required
Realised risk	Identified risks that have been realised and corrective actions taken	As required

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. Communications channels also should ensure personnel can

communicate risk-based information across department units, processes or functional silos. In most cases, normal reporting lines in a department are the appropriate channels of communication. In some circumstances, however, separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative. Whatever channels of communication are used, it is imperative that personnel understand that there will be no reprisals for reporting relevant information.

External communications channels can provide highly significant input on the design or quality of products or services. Management considers how its risk tolerance aligns with those of its customers, suppliers and partners, ensuring that it does not inadvertently take on too much risk through its department interactions.

COMPONENT 8: MONITORING

The Departments risk management changes over time and accordingly must be monitored and reviewed on a regular basis. Risk responses that were once effective may become irrelevant; control activities may become less effective; or no longer be performed; or entity objectives may change. This can be due to the arrival of new personnel, changes in entity structure or direction, or the introduction of new processes. In the face of such changes, management needs to determine whether the functioning of each enterprise risk management component continues to be effective. The Risk Management unit will conduct progress reviews to monitor the implementation of risk action plans.

Risk should be regularly monitored – a process that also includes assessing both the presence and functioning of risk management. Monitoring can be performed in two ways: through ongoing activities or separate evaluations. This will ensure that risk management continues to be applied at all levels and across the organisation.

Ongoing monitoring should be built into normal, recurring operating activities of the department, should be performed on a real-time basis and should react dynamically to changing conditions and is ingrained within the department. As a result, it is more effective than separate evaluations. Since separate evaluations take place after the fact, problems often will be identified more quickly by ongoing monitoring routines.

The frequency of separate evaluations is a matter of management's judgement, although there should be one overall risk evaluation at least annually.

In making that determination, consideration should be given to the nature and degree of changes, form both internal and external events, and their associated risk management strategies and related controls and the results of the ongoing monitoring.

Usually, some combination of ongoing monitoring and separate evaluations will ensure that risk management maintains its effectiveness over time.

Risk Appetite, Risk Bearing Capacity and Risk Tolerance

The risk appetite, bearing capacity and tolerance levels will be determined in accordance with the Risk Appetite Framework of the Department.

RISK MANAGEMENT ACTIVITIES AS APPLIED TO PROJECT MANAGEMENT

In project management, risk management includes the following activities:

- Plans should include risk management tasks, responsibilities, activities and budget.

- Assigning a risk officer, a team member other than a project manager who is responsible for foreseeing potential project problems.
- Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally a risk may have an assigned person responsible for its resolution and a date by which the risk must be resolved.
- Creating anonymous risk reporting channel. Each team member should have possibility to report risk that he/she foresees in the project.
- Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by who and how will it be done to avoid it or minimize consequences if it becomes a liability.
- Summarizing planned and faced risks, effectiveness of mitigation activities, and effort spent for the risk management.

RISK MANAGEMENT FOR MEGAPROJECTS

Megaprojects (sometimes also called "major programs") are extremely large-scale investment projects. Megaprojects include bridges, tunnels, highways, railways, power plants, dams, wastewater projects, public buildings, information technology systems. Megaprojects have been shown to be particularly risky in terms of finance, safety, and social and environmental impacts. Risk management is therefore particularly pertinent for megaprojects and special methods and special education have been developed for such risk management.

RISK MANAGEMENT AND BUSINESS CONTINUITY MANAGEMENT/PLAN

Risk management is simply a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore, all organizations have to accept some level of residual risks.

Whereas risk management tends to be pre-emptive, Business Continuity Plan (BCP) was invented to deal with the consequences of realized residual risks. The necessity to have BCP in place arises because even very unlikely events will occur if given enough time. Risk management and BCP are often mistakenly seen as rivals or overlapping practices. In fact, these processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP (assets, impact assessments, cost estimates etc.). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process. However, the BCP process goes beyond risk management's pre-emptive approach and assumes that the disaster will happen at some point.

6. ASSURANCE ACTIVITIES

The Internal Audit division shall include, in their audit plan the examination of the departmental risk environment taking into consideration the identified risks of the department. Internal Audit shall from time to time issue reports to the Accounting Officer indicating progress made with regard to the risks identified. Should the Office of the Head: Culture, Sport and Recreation elect not to rely on tests performed by the internal audit, they may re-examine the department's risk environment.

COMBINED ASSURANCE can be defined as the planned approach to assess the extent and adequacy of assurance coverage on key organisational risks.

King IV defines Combined Assurance as:

Integrating and aligning assurance processes in an organisation to maximise risk and governance oversight and control efficiencies and optimise overall assurance to the Audit Committee and Risk Committee, considering the institution's Risk Appetite.

The combined assurance has been designed to highlight the relevant high-risk areas and the assurance to be provided by management, External Audit, Internal audit and other consultants or service providers in order for the Executive Authority to be appraised of the Risk management efforts undertaken to manage the risks to acceptable level.

- Combined assurance should be based on identified risks and how they are managed.
- Assurance is achieved and reported to the Accounting Authority.

It must be linked to Risk management Activities to assist the Accounting Officer to review the effectiveness of the Risk Management systems.

Combine Assurance Plan will be designed to highlight relevant high-risk areas and the assurance to be provided by Management, External Audit, and Internal Audit. The Department will compile a plan based on the analysis of the identified risks to enable management to assign resources priority efficiently to mitigate the risks to an acceptable level and to identify who is responsible for each risk to ensure that risk exposure is appropriately mitigated.

7. MONITORING OF ACHIEVEMENT OF THE RISK MANAGEMENT STRATEGY

Management of the Department of Culture, Sport and recreation acknowledges that in order to realize the full potential, risk management processes and strategy should be subject to periodic reviews. Senior management of the department shall ensure that risk management strategy monitoring forms part of the agenda of the senior management meeting and also the Risk Management implementation Plan forms part of the Performance Agreement of the Executive Management of the Department. Quarterly monitoring and reporting of progress against the action plans developed to treat risks shall take place as scheduled. Quarterly progress report shall be submitted to the Audit Committee.

THE RISK MATURITY LEVEL EVALUATION

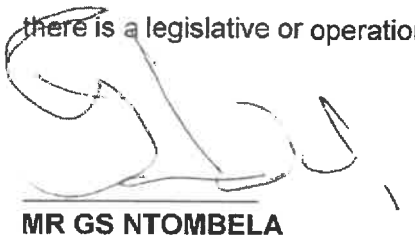
DCSR RISK MANAGEMENT MATURITY –LEVEL ASSESSMENT TOOL

The Risk Maturity Methodology of DCSR focuses on a structured collection of elements and components of Risk Management as contained in "The Committee of Sponsoring Organizations of the Treadway Commission, 2004- Enterprise Risk Management Integrated Framework), namely:

COMPONENT	ELEMENT
1. Internal Environment	• Risk Management Philosophy • Corporate Governance • Responsibility • Competence • Integrity and ethical values
2. Objective Setting	• Strategy formulation • Strategy Implementation • Strategy Effectiveness
3. Event Identification	• External factors driving events • Internal factors driving events • Events affecting business and strategies • Event characteristics
4. Risk Assessment	• Assessment metrics • Assessment methods
5. Risk Response	• Risk mitigation strategies
6. Control Activities	• Control basis • Controls over objectives • Controls over processes • Controls over information processing
7. Information and Communication	• Information over objectives • Information quality • Information management • Communication
8. Monitoring	• Monitoring activities • Monitoring corrective actions

8. APPROVAL

This policy takes effect from the day of approval. This policy will be subjected to review or as and when there is a legislative or operational change. This will be done through consultation with all stakeholders.



MR GS NTOMBELA
HEAD: CULTURE, SPORT & RECREATION
30 / 04 /2024

ANNEXURE A

Integrating risk management and planning process (RMPP)

The developed risk management planning process includes a sequence of activities that will culminate in every financial year. The RMPP is limited but focused set of strategic objectives that are shared by all employees within the Department of Culture, Sport and Recreation (DCSR) and inform the risk management planning process. The planning process links risk management with the day-to-day activities of Units within DCSR

Risk Management planning process:

Dates	Activity
May – early July	DCSR conducts risk management planning activities. Objectives are identified. The risks to those objectives are identified. This must be done before the department submits their budget to Treasury.
Mid July – September	DCSR shall ensure that risk management plan is integrated in both, the strategic and operational plans.
End October – Mid January	DCSR shall ensure that Risk Management plan is still aligned with the operational and strategic plan. The identified risks should be evaluated and prioritized. These activities constitute the Risk Assessment process.

ANNEXURE 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, the inherent risk, the perceived effectiveness of existing controls, as well as the residual risk remaining.

Qualitative assessment of impact

Impact	Consequence	
Catastrophic	Negative outcomes or missed opportunities that are of critical importance to the achievement of objectives.	5
Major	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet the objectives	4
Moderate	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives.	3
Minor	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives.	2
Insignificant	Negative outcomes or missed opportunities that are likely to have negligible impact on the ability to meet objectives	1

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. The risk is already occurring, or is likely to occur more than once within the next 12 months	5
Likely	More than an even chance of occurring. The risk could easily occur, and is likely to occur at least once within the next 12 months	4
Possible	Could occur quite often. There is an above average chance that the risk will occur at least once in the next 3 years	3
Unlikely	Small likelihood but could happen. The risk occurs infrequently and is unlikely to occur within the next 3 years	2
Rare	Not expected to happen – Event would be a surprise. The risk is conceivable but is only likely to occur in extreme circumstances	1

Inherent risk exposure

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

Inherent Risk Rating	Inherent Risk Magnitude	Risk Acceptability	Proposed mitigating steps
20 - 25	Maximum risk	Unacceptable risk	Take action to reduce risk with highest priority
15 - 19	High risk	Unacceptable risk	Take action to reduce risk with highest priority
10 - 14	Medium risk	Unacceptable risk	Take action to reduce risk, inform management
5 - 9	Low risk	Accept Risk	No risk reduction – control, monitor, inform management
1 – 4	Minimum risk	Accept Risk	No risk reduction – control, monitor, inform management

Residual risk exposure

The table below was used to categorise the residual risk exposure:

Category	Risk tolerance	Factor
Unacceptable	The risk is intolerable and requires urgent action to further mitigate the exposure	15 - 25
Cautionary	The risk exposure exceeds the current risk tolerance and should be monitored to ensure prompt intervention if and when required	10 - 14
Acceptable	The risk exposure is tolerable	1 - 9