agriculture & rural development

Department of
Agriculture and Rural Development
FREE STATE PROVINCE

# RISK MANAGEMENT UNIT

# RISK MANAGEMENT STRATEGY

# TABLE OF CONTENTS

# 1. INTRODUCTION

This document is prepared to provide guidance and direction or describe the methodology to be followed by the risk management unit of the Free State Department of Agriculture and Rural Development in the performance of their risk management activities. It is based on best practices of risk management standards and is intended to give guidance as to how to approach and implement risk management strategies in the Department, starting from the planning, identification and assessment of risks, reporting, follow up and monitoring phases.

While it will give guidance on various decisions, which must be made throughout the process, it will not address every aspect thereof. The official must use professional judgement to adapt the procedures defined in this guideline to the circumstances of each project.

The mission of the risk management unit is to enable effective governance, administration and service delivery, through adherence to optimal enterprise risk management practices.

The vision is to provide enterprise risk management support service enabling more effective governance within the Department of Agriculture and Rural Development.

## 2. BACKGROUND

In terms of the Public Finance Management Act, Section 38(1)(a)(i), the accounting officer must ensure that the department, trading entity or constitutional institution has and maintains effective, efficient and transparent systems of financial and risk management and internal control.

Treasury Regulations 3.2.1 extends the above requirement by putting emphasis on Risk Assessment, Risk Management Strategy and Fraud Prevention Plan and can be summarized as follows:

(i) The Accounting authority must ensure that a risk assessment is conducted regularly to identify emerging risk of the institution.

(ii) A 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.

(iii) The strategy must be clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the institution.

The King III Report on Corporate Governance for South Africa, applicable to both private and public environments, recommends that a dedicated committee (Risk Management Committee) be established to assist in reviewing the management of risks that face the department.

It is against this backdrop of legislation and good corporate governance practices that the department has established a Risk Management Unit.

The scope of work of the risk management unit is to determine whether the systems of risk management are adequate and functioning in the following manner:

- The development of Risk Management Methodologies and a Financial Governance Framework and training manuals;

- Training of junior, middle and senior management;

- Establishing Risk Management, inclusive of Internal Control capacity within the department; and

- The embedding of governance and risk management practices into normal management processes.

The Risk Management unit does not relieve management of its primary responsibility for establishing and supporting an adequate control environment within their areas of responsibility.

## 3. AUTHORITY, PURPOSE AND RESPONSIBILITY

The authority, purpose and responsibility to undertake risk management is derived from section 38(1) (a) (ii) of the Public Finance Management Act (PFMA), Act No 1 of 1999 as amended by Act No. 29 of 1999, and chapter 3 of the Treasury Regulations issued under this Act which state that, "The accounting authority must ensure that a risk assessment is conducted regularly so as to identify emerging risks of the department. A 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 strategy must be clearly communicated to all employees to ensure that the risk management strategy is incorporated into the language and culture of the department."

The responsibility for managing risks is not restricted to any one person or group of specialists, it is the duty of every official in the Department of Agriculture and Rural Development.

## 4. RISK MANAGEMENT COMMITTEE

A Risk Management Committee (RMC), appointed by the Accounting Officer, is responsible to assist Accounting Officer in discharging his/her risk management responsibilities and accountability for risk management in accordance with prescribed legislation and corporate governance principles. The RMC is accountable to the Accounting Officer and operates in terms of the approved RMC Charter.

## 5. APPROACH

The Department of Agriculture and Rural Development utilises the Public Sector Risk Management Framework published by National Treasury for the effective and efficient provision of Risk Management in the department. The department also applies the Committee of Sponsoring Organisations of the Treadway Commission's framework (COSO) that could be used by management to evaluate and improve the department's enterprise risk management. Enterprise Risk Management (ERM) applies risk management throughout the organization rather than only on selected business areas or disciplines. This provides key principles and concepts, a common language and clear direction and guidance. The framework is geared to achieving entity objectives.

Enterprise risk management consists of interrelated components, derived from the way management runs the department. These components are integrated with the management process. There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them.

# 6. METHODOLOGY FRAMEWORK

## 6.1 Background and Overall Objectives

Accounting Officers should ensure that they have effective, efficient and transparent systems of financial and risk management and internal control. This responsibility is also assigned to other officials within the department and their respective sections and includes:

- The responsibility to ensure the effective, efficient, economical and transparent use of financial and other resources within that official's area of responsibility, and
- The management, including the safeguarding of assets and management of the liabilities, within that official's area of responsibility.

In order to assist the Accounting Officers and officials in discharging certain of their risk management responsibilities in relation to the above, the departments should embark on a process to:

- Identify, characterize, and assess risks or threats,
- Identify ways to mitigate or reduce those identified risks,
- Prioritise risk reduction measures based on strategy,
- Assist the respective officials in the execution of their risk management responsibilities,
- Ensure that the results of the risk assessment or profiling exercise forms the basis of an on-going review and re-rating process by the sections across the Departments,
- Assist the Internal Audit Function in focusing their resources on risk areas identified as being of the most significance i.e. to assist in the determination of the scope of the internal audit work.

**Benefits of Risk Management**

The following benefit flow from an effective risk management process:

- Proactive response to threats
- Better/ Quality decision-making
- Increased awareness, transparent evaluation and sound mitigation of risks
- As a management tool, an integrated risk management framework assists in achieving

objectives more efficiently

- Focuses management on understanding the nature of the risks and ensures that management takes steps to mitigate the potential negative consequences
- Allows management to evaluate, prioritise and address the critical risks and channel resources to these risks, ultimately improving the utilisation of resources to address critical risks.

## 6.2 Components of Enterprise Risk Management

Enterprise Risk Management consists of eight interrelated components derived Enterprise risk management consists of eight interrelated components derived from the way management runs the Department. These components are integrated with the management process. There is a direct relationship between objectives, which are what the Department strives to achieve, and enterprise risk management components, which represent what is needed to achieve them thus it is imperative that Risk management is not undertaken in isolation but rather be integrated with other management processes of the Departments. This relationship is depicted in a three-dimensional matrix, in the form of a cube.


The eight step risk management process the Department will adhere to are as follows:

- **Internal Environment** - The internal environment encompasses the tone of an organisation, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective Setting** – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite. The setting of these objectives is usually completed during the "strategic planning and budgetary process."
- **Risk/ Event Identification** – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channelled back to management's strategy or objective-setting processes.
- **Risk Assessment** – Risks are analysed, considering likelihood and impact, as a basis for

determining how they should be managed. Risks are assessed on an inherent and a residual basis.

- **Risk Response** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- **Control Activities** – Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly and in a timely manner. Control activities are part of the process by which the departments strive to achieve their business objectives. Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- **Information and Communication** – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- **Monitoring** – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both. This will ensure that risk management continues to be applied at all levels and across the Departments.

# 7. PROCESS FLOW

Generally, the process of a risk management consists of four interwoven phases:

## 7.1. Planning

This phase unfold the internal environment as governance principles within the risk management unit and it relates to the designing and implementation of policies and strategies in respect of transparent, effective and efficient risk management processes. It further focuses on gathering information on the planning of the risk management activities which includes:

- Review of risk management policy and strategy,
- Risk management implementation plan, and
- Other planning documents.

Planning of projects may begin with an opening/entrance meeting being held which is an important step in the risk assessment process. It is an opportunity to establish the proper tone and to begin building good relationships. Explain who, what, where, when, why, and how for those who are unfamiliar with the risk assessment process. The main purpose of the meeting is to determine what their expectations are regarding the risk assessment process and also to clarify that the role of the risk management unit is to facilitate the process and not to own it. The scope of the assessment is also agreed upon.

A planning memorandum is drawn up which places the expectations of both the client and the unit in writing and dates upon which different phases is to be completed and agreed upon.

This process facilitates the gathering of information which will enable the unit to learn more about the department, directorate or project.

The unit will also be seeking to identify the focus area's objectives. Key objectives are generally determined through discussion with management and review of a variety of documents

including the strategic plan, mission statement business plans, management reports, budgets etc.

### 7.2. Identification and assessment of risks

This phase refers to the objective setting, event identification and the risk assessment components of COSO. This phase will focus the process to identify and rate risks. The risk identification process must identify unwanted events, undesirable outcomes, emerging threats, as well as existing and emerging opportunities on a continuous basis. By virtue of the department\s existence, risks will always prevail, whether the Institution has controls or not.

When identifying risks, it is also important to bear in mind that "risk" also has an opportunity component. This means that there should also be a deliberate attention to identifying potential opportunities that could be exploited to improve departmental performance. In identifying risks, consideration should be given to risks associated with not pursuing an opportunity. The initial stage is to identify strategic risks. This is done through a risk assessment workshop which focuses on the following components of the framework:

- **Objective Setting** – Objectives must exist before management can identify potential events that may have an impact on the achievement of these objectives
- **Event Identification** – Internal and external events affecting achievement of an entity's objectives (distinguishing between risks and opportunities); and
- **Risk Assessment** – Risks are rated on their impact, if materialised, and likelihood of materialising.

#### (i) Risk Assessment Workshop Flow

- Identify the organisation's **objectives** and classify them as;
    - Strategic – high-level goals, aligned with and supporting its mission;
    - Operations – effective and efficient use of its resources;
    - Reporting – reliability of reporting; and
    - Compliance – compliance with applicable laws and regulations
- Identify **events** (risk or opportunity) that may have an impact on the achievement of said

objectives and group them into categories such as;

- Physical and operational;
- Human resources;
- Technology;
- Business continuity and disaster recovery;
- Financial, credit and market;
- Compliance.

- Agree on the **criteria** that would be used to evaluate the impact of an event and the likelihood that the event may materialise;
- Rate the **current** impact and likelihood that an event may have on the achievement of an objective;
- Identify **controls** that may mitigate the impact or likelihood that an event may materialise. Controls should be considered o the basis of :
  - **Design effectiveness** – Is the control "fit for purpose" in theory i.e. is the controls designed appropriately for the function for which it is intended
  - **Operational effectiveness** – Does the control work as practically intended.
- Group the **controls** as follows:
  - Preventative;
  - Detective;
  - Corrective; or
  - Risk responses.
- Rate the **desired** impact and likelihood that an event may have on the achievement of an objective.

The criteria for measuring the impact of a risk materialising and likelihood that a risk may materialise should be agreed by the participants of the workshop.

The impact for the department has been defined as the potential loss to the organisation or the service delivery failure should the risk materialise. Likelihood has been defined as the probability that an event, which could have an impact on the organisation achieving its objectives, may occur.

**Risk Assessment** – Risks are evaluated on an inherent (prior to consideration of controls) and residual basis (after consideration of controls). Risks are rated considering:

- Current likelihood and impact,
- Possible controls that may mitigate these risks; and
- The desired likelihood and impact.

Excel spreadsheets are used to capture the inputs of participants during a risk assessment workshop and generate the reports included in the detailed risk register.

Risk assessments should be performed through a three stage process:

- Firstly, the inherent risk should be assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk;
- Secondly, a residual risk assessment should be performed to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk; and
- Thirdly, the residual risk should be benchmarked against the department's risk appetite to determine the need for further management intervention, if any.

**The Risk Assessment process includes 4 steps:**

**Step 1**: Quantifying the parameters (scoring system) of impact and likelihood before the actual assessment.

**Impact**

Potential loss to the department or service delivery failure should the risk materialize.

| | Rating | Definition | | |
|---|---|---|---|---|
| | | Value (Rand) | Reputation | Time |
| 1 | Insignificant | R0 – R5 000 | Internal | 1 – 2 Days |
| 2 | Minor | R5 001 – R20 000 | Local Press | 1 – 4 Weeks |
| 3 | Moderate | R20 001 – R100 000 | Provincial Press | 1 – 3 Months |
| 4 | Major | R100 001 – R500 000 | National Press | 3 – 6 Months |
| 5 | Critical | Above R500 000 | International Press | >6 Months |

## Likelihood

The probability that an event, which could have an impact on the department achieving its objectives may occur.

| | Rating | Definition |
|---|---|---|
| 1 | Rare | <10% |
| 2 | Unlikely | 10% - 25% |
| 3 | Moderate | 25% - 50% |
| 4 | Likely | 50% - 90% |
| 5 | Common | >90% |

- A risk is allocated a risk rating based on the assessment of its impact and likelihood
- The risk rating index is utilized to determine the extent of the risk exposure the institution is faced with in order to allocate the appropriate response to that specific risk.

Example: likelihood score X impact score = risk rating

5 X 3 = 15

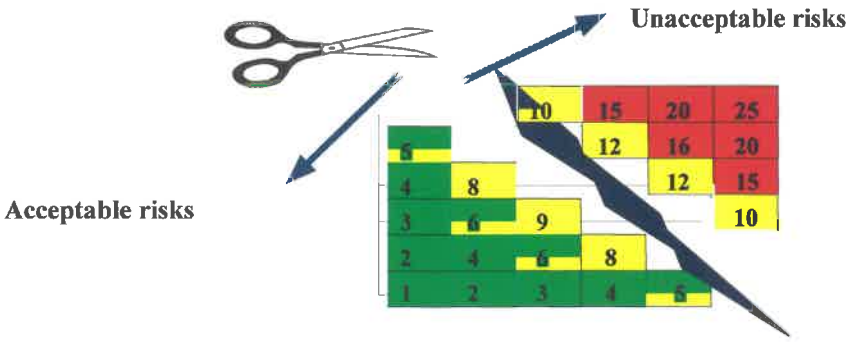
**Step 2:** Applying the parameters to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium or low risk

**Risk index = impact x likelihood**

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

| Risk index | Risk Magnitude |
|---|---|
| 15 - 25 | High risk |
| 8 - 14 | Medium risk |
| 1 - 7 | Low risk |

**Step 3:** Determining the risk acceptance criteria by identifying what risks will not be tolerated




**RESIDUAL RISK**

Residual risks are the risks that are identified after taking into consideration the effect and impact of direct, existing control measures implemented as well as the impact of compensating control measures, relative to a risk identified.

Likelihood represents the possibility that a given event will occur, while impact represent its effect should it occur. Estimates of risk likelihood and impact often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimate. Internally generated data based on the department's own experience may reflect less subjective personal bias and provide better results that data from external sources.

The mitigation effectiveness is carefully considered and determined in order to moderate the risk exposure.

**Mitigation Effectiveness Ratings**

| Category | Outcome Description | Rating % / Factor |
|---|---|---|
| Very Good | Could not be more effectively implemented to mitigate risk | 90% |
| Good | More risks are effectively mitigated | 70% |
| Satisfactory | There is room for some improvement | 50% |
| Weak | Some risks appear to be mitigated but there are some deficiencies | 30% |
| Unsatisfactory | Mitigation is effective | 10% |
| **Residual risk – considered controls (level of exposure) : IR x (I –CE) = RR** | | |

**Step 4:** Determine risk acceptability and what action will be proposed to reduce the risk

## Risk Appetite

The Department of Agriculture and Rural Development is exposed to a variety of risks as it strives to achieve the objectives set out in its APP and Strategic Plan. This risk appetite statement describes the level at which risks are acceptable /unacceptable and where strategies must be implemented to manage risk. The following table presents the overall risk appetite statement of the department:

| Risk Index | Risk Magnitude | Risk Acceptability/ Appetite | Proposed Actions |
|---|---|---|---|
| 15 -25 | High Risk | Unacceptable | Take action to reduce risk with highest priority, Accounting Officer attention<br>Poor design and implementation of controls |
| 8 – 14 | Medium Risk | Unacceptable | Take action to reduce risk, Inform Senior Management<br>Some redesign of control if needed/ improvement on implementation |
| 1 - 7 | Low Risk | Acceptable | Low level of control intervention required, if any<br>No risk reduction- control, monitor, inform management |

**Risk Assessment Results**

The results of the risk assessment process represent the participants' interpretation and perception of the nature and quantum of the risks impacting the organisation. The quality of the results therefore depends on the knowledge, experience and quality of inputs from the participants. The objective of this task is to assess risk before considering the effect of controls and other risk mitigation actions through a systematic methodology. Inherent business risk reflects of two elements, impact and likelihood of occurrence. By measuring these two factors, risks can be prioritised with greatest emphasis generally directed toward the high impact/high likelihood.

### 7.3. Control activities or action plans

**Risk Response** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite. The department develops risk responses for all material risks whether or not the management thereof is in direct control of the department.

**Control Activities** – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

**Potential risk treatments**

Once risks have been identified and assessed, all techniques to manage the risk into one or more of these four major categories:

- Avoidance (eliminate)
- Reduction (mitigate)
- Transfer (outsource or insure)
- Acceptance

Ideal use of these strategies may not be possible. Some of them involve trade-offs that are not acceptable to the organisation or person making the risk management decisions. Another source calls these categories **ACAT,** for Avoid, Control, Accept, or Transfer.

**Risk avoidance**

This strategy involves not performing an activity that could carry risk. For example, choosing a different strategy or terminating the activity that produces the risk.

**Risk reduction/ control**

This strategy involves implementing controls that reduce the severity of the loss or the likelihood of the loss from occurring. It is also known as risk treatment or optimisation by implementing or improving the internal control system. Acknowledging that risks can be positive or negative, optimising risks means finding a balance between negative risk and the

benefit of the operation or activity, and between risk reduction and effort applied.

Outsourcing could be example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. .

**Risk Acceptance**

The risk acceptance strategy involves accepting the loss or benefit of gain, when it occurs. It also involves taking the risk by performing the activity in the absence of controls.

**Risk Transfer**

This strategy involves transferring the activity to a third party or sharing the burden of loss or the benefit or gain, from a risk, and the measures to reduce a risk with another party. For example contracting out of services, establish strategic partnerships and buying insurance.

**Create a risk management plan**

Management is responsible for designing, implementing and monitoring the effective functioning of the system internal controls. Management should select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level of management. For example, a risk concerning the image of the department should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management action plan/ mitigation plan should propose applicable and effective controls for managing the risks.

The risk management action plan/ mitigation plan will contain a schedule for control implementation and responsible persons for those actions. This information will be detailed in the department's risk registers.

**Implementation**

Corrective actions detailed in the risk management action/ mitigation plans in the risk registers for mitigating the effect of the risks should be implemented according to timeframes decided

upon.

**Review and evaluation of the plan**

Initial risk management plans will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decision to be made in dealing with the risks being faced.

Risk analysis results and management plans will be updated periodically. There are two primary reasons for this:

- To evaluate whether the previously selected security controls are still applicable and effective and;
- To evaluate the possible risk level changes in the business environment.

Any changes to the risk profile of the department will be reported to the Risk Management Committee on a quarterly basis.

**Risk Categories and Descriptions**

| | Risk Category | Description |
|---|---|---|
| 1. | Human Resources | Risks that relate to the human resources of the department. These risks can have an effect on an department's human capital with regard to:<br>• Integrity and honesty<br>• Skills and competence<br>• Retention<br>• Motivation and morale |
| 2. | Knowledge/Information Management | Risks related to the department's management of knowledge and information<br>Example:<br>• Availability of information<br>• Integrity of information and data<br>• Retention<br>• Safeguarding |

| | Risk Category | Description |
|---|---|---|
| 3. | Litigation | **Risk that the department might suffer losses due to litigation and lawsuits against it.**<br><br>Losses from litigation can emanate from:<br>• Claims by employees, the public, service providers and other third parties.<br>• Failure by the department to exercise certain rights that are to its advantage |
| 4. | Asset Management | Risks associated with the misuse, physical damage, theft and under-utilisation and wastage of the department's assets. |
| 5. | Service Delivery | Risks related to the disruption, quality, denial, non-availability or quality of service delivery to the public. |
| 6. | Technology/IT | The risk that relate specifically to the department's IT objectives, infrastructure and requirements.<br><br>Relevant aspects include:<br>• Security concerns<br>• Technology availability (uptime)<br>• Technology effectiveness<br>• Hardware obsolescence<br>• Changes in technology |
| 7. | Third Party Performance | Risks related to the department's dependence on the performance of a third party.<br><br>Risk in this regard is the likelihood that a service provider might not perform according to an agreement entered into with the department.<br><br>Non-performance could include:<br>• Outright failure to perform<br>• Not rendering the required service in time<br>• Not rendering the correct service<br>• Inadequate/poor quality of performance |
| 8. | Health and Safety | Risks related to occupational health and safety issues and concerns (e.g. deaths and injuries on duty, accessibility of facilities to persons with disabilities, etc.) |

| | Risk Category | Description |
|---|---|---|
| 9. | Disaster Recovery | Risks related to the department's degree of preparedness or absence thereto, natural disasters that could impact the normal functioning and continuity of the business operations e.g. natural disasters, acts of terrorism etc.<br>Factors to consider include:<br>• Disaster management and business continuity procedures, and<br>• Contingency planning |
| 10. | Compliance/regulatory | Risks related to possible breaches to legislation, prescripts and regulations which the department should comply with.<br><br>Aspects to consider in this regard are:<br>• Failure to monitor or enforce compliance<br>• Monitoring and enforcement mechanisms<br>• Consequences of non-compliance |
| 11. | Fraud and corruption | Risks associated with fraud and corruption practices, both by staff and external parties.<br>These include:<br>• Misrepresentation for the purposes of concealing illegal acts<br>• Collusion<br>• Offering and/or acceptance of kickbacks<br>• Nepotism |
| 12. | Financial | Risks encompassing the entire scope of general financial management.<br>Potential factors to consider include:<br>• Cash flow adequacy and management thereof<br>• Financial losses<br>• Financial statement integrity<br>• Revenue collection<br>• Financial planning |
| 13. | Cultural | Risks relating to the department's overall culture and control environment.<br>The various factors related to organisational culture include:<br>• Communication channels (the existence and the effectiveness & efficiency thereof)<br>• Cultural integration<br>• Entrenchment of ethics and values<br>• Goal alignment<br>• Leadership and management style |

| | Risk Category | Description |
|---|---|---|
| 14. | Reputation | Factors that could result in the tarnishing of the department's reputation, public perception and corporate image. |
| 15. | Economic | Risks related to the department's economic environment |
| 16. | Political | Risks emanating from political factors and decisions that have an impact on the department's mandate and operations |
| 17. | Natural environment | Risks related to the adverse natural environment consequences of executing the department's strategy.<br>Factors to consider include:<br>• Depletion of natural resources<br>• Environmental degradation<br>• Environmental contamination |

### 7.4. Reporting

The reporting phase is crucial as it is the deliverable of the entire process and effectively begins the process of implementation of the mitigation of identified risks.

Risk communication is a complex cross-disciplinary academic field. Problems for risk communicators involve how to reach the intended audience, to make the risk comprehensible and relatable to other risks, how to pay appropriate respect to the audience's values related to the risk, how to predict the audience's response to the communication, etc. The main goal of risk communication is to improve collective and individual decision making. Risk communication is somewhat related to crisis communication.

The report communicates the results of the work and for that reason alone it is perhaps one of the most important parts of the process. It is important because it is what the department and senior management sees, and is the only product of our work that management receives. If written and communicated well, it can act as a positive change agent prompting management to take corrective action.

The report should contain the following summary:

- List of organisational objectives;
- List of risks with their current and desired impact and likelihood; and

- List of controls that participants believe to be in place to mitigate risks.

**Summarise Results and Map to Units**

Risk summaries based on the rating of risks before the consideration of controls (inherent risk) and after consideration of controls (residual risk) are important. Most readers of a report and more importantly, key decision makers, tend to focus on the summary and may delegate the detailed consideration of the report to other staff. Consequently risk summaries represent the best opportunity to communicate the significant matters arising from the report. A summary that is colour coded to correspond with high, medium and low risk (i.e. the heat map approach) should be used. The mapping of the risks provides an immediate visual and outlines where the risks lie on a graph which enables the reader to identify and prioritise which are the high risks require immediate action and which ones do not require corrective action.

The objective of the risk summary is to facilitate management validation of the risks identified and to facilitate prioritising the risks for purposes of strategic planning.

Generally, two heat maps should be compiled for the department. One based on all the risks of the organisation as a whole and one which maps risks cased on the different directorates of the department. The heat map based on the directorates can facilitate the setting of priorities during the strategic planning process.

## Example of Risk Heat Map

| Likelihood | | | | | | |
|---|---|---|---|---|---|---|
| | Common (5) | | | | | SS2; SS3; PPOS5;PPOS6; HRM1; FMS1;FMS2;FM1; FM3; ABDS1 |
| | Likely (4) | | | | IA2; PPOS2; HRM2; LC1; FSD1; EAS1; FS1; VPH1; TTS1; FET2 | IA3; SS1; LS1; FM2; FM4;RM1; RM2;CS1;CS2; CS3; LC2; DRM1; DRM2; AH1;AH2; EC1; MES1;HET2 |
| | Moderate (3) | | | IA1; IA4; IA5; AH3; HET1; FET1; FET3 | PPOS3; PPOS4; RS1 | ENG2; ENG3; VLS1; ISS1; ABDS2 |
| | Unlikely (2) | | | PPOS1 | | ENG1 |
| | Rare (1) | | | | | |
| | | **Insignificant (1)** | **Minor (2)** | **Moderate (3)** | **Major (4)** | **Critical (5)** |

A risk register containing details of all the risk should also be included in the report so that it may be used as a reference moving forward.

The risk assessment process does not end with the issuing of this report. The report will give management an opportunity to study the risks identified and thereafter the process of action plans should begin. Action plans are control activities that will need to be put in place by management in order to ensure that risks are mitigated to an acceptable level. Plans should be action-oriented, specify a date by which the action will be implemented and who the responsible person is.

Management will also be required to provide reports on a periodic basis where they should

outline whether actions have been taken at the set dates and what the progress is.

### 7.5. Follow up and monitoring

This phase is arguably the most important phase as this is where the unit will get an opportunity to determine whether risk management has the desired impact or not.

The follow up and monitoring phase is the most important phase in the whole process. This is due to the fact that this is ultimately when the risk management unit can assess whether risks are being mitigated effectively throughout the department.

The unit should perform follow up and monitoring on a quarterly basis where the results of action plans are assessed and corrective action is taken regarding those plans which are not effective.

This phase also encourages management to take ownership and responsibility of their risk as they are the risk owners. The message to be communicated is that the unit is not responsible for the mitigation of risks but is there to facilitate and to ensure that the correct actions are being taken.

### 7.6 Tools

The BarnOwl software will be used as the tool to capture the inputs of participants of the workshop, generate reports and maintain the risk register. Managers will be trained on the use of the software to enable them to contribute and effectively manage the risks in their area of responsibility.

## 8. REVIEW OF RISK MANAGEMENT STRATEGY

The Risk Management Strategy shall be reviewed when deemed so necessary to ensure its continued application and relevance. Amendments will, as soon as reasonably possible, be submitted to the Accounting Officer for approval and brought to the attention of all officials for its implementation.

## 9. RECOMMENDATION AND APPROVAL

It is hereby recommended that approval for the Risk Management Strategy be granted to ensure best practices of risk management standards and the approach to implement risk management strategies in the department.

**REVIEWED BY:**

**MS. T CRISP**
**CHIEF RISK OFFICER**

**DATE:** 26/03/2018

**THE RISK MANAGEMENT COMMITTEE HAS REVIEWED AND RECOMMENDS THE APPROVAL OF THIS RISK MANAGEMENT STRATEGY:**

**MR. D NKAISENG**
**CHAIRPERSON**

**DATE:** 27/03/18

**THE HEAD OF DEPARTMENT HAS REVIEWED AND APPROVES THIS RISK MANAGEMENT STRATEGY:**

**MR. MP THABETHE**
**HEAD OF DEPARTMENT**

**DATE:** 29/03/2018