Risk Management
– Guide –

environmental affairs

Department:
Environmental Affairs
REPUBLIC OF SOUTH AFRICA

CONTENTS

1. FOREWORD

The concept of risk management is not new to the public service,in that the basic principles of service delivery (Batho Pele, 1997) clearly articulate the need for prudent risk management to underpin the achievement of Government's objectives.

The DEA Enterprise Risk Management Handbook forms the basis of our efforts to improve the risk management capability of the DEAin support of achieving a risk intelligent culture.

We need to enhance our capability to identify, manage and monitor those risks at a strategic, operational and process level that may impact (positively and negatively) on the DEA achieving its mandate and strategic intent.

Further, it is important for all of us to understand that the responsibility for risk management vests at all levels of management and is not limited to only the accounting officer, the Enterprise Risk Management Directorate and Internal Audit.Therefore, the decision-making processes of the DEA must at all times consider both risk and reward whilst meeting the needs and expectations of our stakeholders and partners.

The handbook provides a structured and uniform approach for achieving the above.

Mr Alf Willis

Director General (ACTING)

Date: 19/06/2013

1. INTRODUCTION

1.1 Purpose

The DEA Enterprise Risk Management Guide represents the source of reference and guidance for management and staff on the governance, implementation and execution of risk management within the organisation.

The Guide's purpose is to create a structured and consistent approach to risk management, aligning strategy, processes, people, technology and information systems for the purpose of evaluating and managing the uncertainties that the DEA faces due to the nature of the business, the change in environment, legislation and control environment.

Starting from the premise that risk is an unavoidable consequence of any organisation's activities, the aim of the Guide is to provide the overall direction within which management and employees can operate in order to embed a strong risk management culture throughout the DEA.

The Guide outlines the DEA's beliefs about risk and how it chooses to manage risk and reflects the value that the DEA seeks. The Guide details the commitments the DEA has made to Enterprise Risk Management (ERM) and the approach to be followed in implementing ERM and managing risks. This Guide provides the foundation for creating a culture of risk management in the organisation that is embedded in all its operational processes.

This Guide further serves as a base to set objectives regarding the level of ERM performance and responsibility that the DEA shall strive to achieve, and against which all ERM activities and operations shall be evaluated.

On a practical level, the Guide also serves to ensure that the results and intelligence provided from the risk management pro-

cesses serve to inform decision-making and priority setting at all levels of the organisation.

Finally, the Guide acknowledges the Public Sector Risk Management Framework and endeavours to align to the principles of risk management recommended within the public sector.

1.2 Structure

This Guide is comprised of the following:

1. DEA Enterprise Risk Management (ERM) Framework (Graphical representation)
2. Guidebooks:
    a) What is risk management
    b) Risk identification
    c) Control activities
    d) Risk assessment
    e) Risk rating
    f) Risk response strategy
    g) Glossary of risk management terminology

DEA ENTERPRISE RISK MANAGEMENT FRAMEWORK

Figure 1: DEA Enterprise Risk Management (ERM) Framework

<table>
<tr><td colspan="6">Enterprise Risk Management (ERM) Framework</td></tr>
<tr><td colspan="6">DEA Strategy</td></tr>
<tr><td colspan="6">1. DEA Enterprise Risk Management</td></tr>
<tr><td>2. Legal Mandate</td><td>4. Structures & Respons-ibilities</td><td>6. ERM Process</td><td>7. ERM Inform-ation System</td><td colspan="2">9. ERM Methodologies (Tools & Techniques)</td></tr>
<tr><td>PFMA
S 38 (1) (a) (i)
S45
Treasury Regulations
Sections 3.2.1, 3.2.7 (a)</td><td>Oversight
Fraud Prevention Committe (FPC), Risk Management Committee (RMC), Audit Committee (AC), Parliamentary Committees National Treasury
Assurance
Internal Audit
Auditor General
Roles and Responsibilities (incl. reporting lines)</td><td>• Establish the contents
• Identify event(s) (inclusive of contributing factors & consequences)
• Communicate positive event to the Strategy function
• Conduct risk assessment
• Develop action plans
• Execute plans
• Monitor, review & reprt on risk mitigation</td><td>8. ERM Reprting</td><td>Information Database(s)

CSA

Root Cause Analysis</td><td>KRI's

Scenario Planning

Risk Assess-ment</td></tr>
<tr><td>3. Policy
Enterprise Risk Management Policy
Fraud Risk Management Policy</td><td>5. Coaching & Training</td><td></td><td>• Risk Registers
• Programme/ unit RM Reports
• Audit Committee
• Fraud Prevention Committee
• Annual Report Disclosure</td><td colspan="2">Risk Analysis Matrix
10. Internal Controls
11. Monitoring & Reviews</td></tr>
</table>

GUIDEBOOK: WHAT IS RISK MANAGEMENT?

1. INTRODUCTION

The term 'risk management' is currently being utilised very liberally within institutions. For example, safety, security, disaster management, business continuity, insurance and internal audit are often referred to as "risk management."

It is certainly true that these functions form part of the wider subject of risk management. But the term 'risk management' means a deliberate focus on all risks of an institution.

The term 'enterprise risk management' (ERM) has become a popular way of describing application of risk management throughout the institution rather than only in selected business areas or disciplines.

Risk management is a management discipline with its own techniques and principles. It is a recognised management science and has been formalised by international and national codes of practice, standards, regulations and legislation.

Risk management forms part of management's core responsibilities and is an integral part of the internal processes of an institution.

This guidebook will use the simpler term 'risk management' and will explain the function in broad terms, showing how the various technical disciplines associated with risk form part of this wider field.

2. DEFINITION

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. This

is not the only definition of ERM as a number of alternative definitions are also used by the ERM community.

The DEA defines risk management as the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects

When properly executed risk management provides reasonable, but not absolute assurance, that the institution will be successful in achieving its goals and objectives.

3. OVERVIEW

Risk management addresses all kinds of material risks to the objectives of the institution. It does not have a bias towards any particular risk control function. Risk management must address all parts of the institution and no part of the institution can claim that they do not need to participate in its processes. Risk management eventually works its way through the entire institution so that all levels of management participate in its processes. Existing risk-related functions such as security risk management, health and safety risk management etc must also align their activities with the institution's risk management plan. This alignment of activities then allows for risk management to reconfigure as ERM.

Many managers have justifiably asked why 'risk' needs a separate focus, and why it cannot be managed as before. The main reason is that the service delivery environment and the public sector's interface with stakeholders have become far more demanding and volatile than before. Historical ways of doing things are no longer effective as evidenced by a number of service delivery and general governance failures. In response to this, the principles of corporate governance and associated legislation require public sector institutions to be more transparent and structured about the ways in which they manage and report on risk.

Stakeholders need to observe that the institution has a proactive and systematic approach to managing organisational risks.

Risk management is recognised by the public sector as an appropriate way of managing risk. Different institutions may have different existing responses to risk, such as safety management and insurable risk to internal control and public relations. It is important that different types of risk receive appropriate attention at an operational or process level. For the institution as a whole, however, stakeholders want to see a single coherent strategy for managing the institution's various risks.

4. WHY DO WE NEED RISK MANAGEMENT?

People often ask why the management of risk cannot remain within the ambit of general management. The truth is that it does, but risk management provides a dedicated focus on risk for the following reasons:

4.1 Corporate governance

Legislation such as the PFMA together with corporate governance codes such as King III expects an institution to implement a risk management plan. As a result of organisational failures in the past, stakeholders do not want to be caught unawares by risk events. They expect that internal control and other risk mitigation mechanisms to be based on a thorough assessment of institution wide risks.

Previously, members of the Accounting Authorities were not involved in the details of risk management because it was regarded as an operational function.

Stakeholders require assurance that management has taken the necessary steps to protect their interests.Corporate governance

thus places the accountability for risk management in the hands of the Accounting Authority / Officer.

Executive Authorities, Accounting Authorities, Accounting Officers and stakeholders now want to know more about the risks facing an institution. This is understandable in an environment of complex and challenging service delivery expectations.

4.2 Planning and organisation

The value of risk management is best leveraged when its principles and techniques are applied during institutional planning processes and organisation. Given the increased levels of volatility and uncertainty, it is vital that plans, particularly multiple year plans, take into consideration a thorough assessment of risks and mitigation strategies.

For this purpose, existing tools and methodologies such as SWOT analysis, PEST analysis, Porters Model and internal reviews can be utilised to supplement the institutions risk management model. Hence, it becomes clear that planning and organisation and risk management are inter-dependent.

4.3 Continuous risk assessment

The risk profile of an institution is fluid, which is to say that it is changing on a continuous basis. Some risks are created by changes initiated by the institution. Others are the result of changes in society, business, legislation or communities.

Even the best management teams will struggle to keep an accurate perspective of changing risks when risk management is approached on an informal basis.

The risk management plan must provide the institution with the ability to systematically identify new and emerging risks, and the

assurance that existing risks are being addressed in the best possible way given the current resource constraints and other challenges.

Change is often beyond the control of management but the risks that it creates needs to be managed.

4.4 Evolution of risk management

Risk management has evolved over recent years. We have seen the integration of risk management techniques with fraud prevention, internal control and corporate governance. There has also been an integration of operational risk management functions into the broader umbrella of enterprise risk management. Aspects such as internal control, safety management, sustainability and environmental management, for example, have increased in importance in recent times. The broadening of risk management has seen a change in emphasis from risks as individual hazards to risks as uncertainties around key objectives.

Risk management has also seen the introduction of new participants into the process. The function is no longer confined to insurance staff, internal auditors, and loss prevention functions.

The wider approach to risk management has brought the function into the view of human resources officers, compliance officers, financial managers, ICT specialists and other functional managers.

4.5 Internal audit plans

internal audit plans are now based on the outcomes of risk assessments. Internal auditors are increasingly basing their priorities on the risk management plan and give priority to high-risk assets and processes.

Internal audit is well-placed to independently validate key controls. The frameworks of internal control used by auditors are useful contributions to the risk management plan.

Internal audit is a key role player in the assurance process with regards to the effectiveness of risk management.

4.6 Cultural adjustment

The essential behaviours of officials charged with responsibility for various activities of risk management must change. This requires a shift in the cultural dynamics insofar as it concerns risk management, which can be achieved through awareness and advocacy, communication, coaching, training and linking to performance measures.

Risk management must be a catalyst for change in behaviour of Managers. Managers need to develop competencies to ensure that they make conscious risk-based decisions. Rather than viewing risk management and its associated activities as mere bureaucracy, managers need to look at it as a powerful driver of service delivery excellence.

5. CONCLUSION

There is a danger that risks that fall outside traditional functions may go unmanaged and have serious consequences on the institutional objectives. The need for broad-based risk management is thus critical as it will also ensure that risks that were not previously given adequate attention are now properly managed. Risk management processes that are integrated within the institution's existing structures are likely to be more effective in producing the desired service delivery and other objectives.

GUIDEBOOK: RISK IDENTIFICATION

1. INTRODUCTION

The purpose of completing a risk identification exercise is to identify, discuss and document the risks facing the institution. Management almost always know what risks the institution is exposed to but they do not always formally record such risks. This necessitated the development of risk identification guidelines to ensure that institutions manage risk effectively and efficiently.

2. THE RISK IDENTIFICATION PROCESS

The objective of risk identification is to generate a comprehensive list of risks based on those events and circumstances that might enhance, prevent, degrade or delay the achievement of the objectives. This list of risks is then used to guide the analysis, evaluation, treatment and monitoring of key risks.

Comprehensive identification and recording is critical because a risk that is not identified at this stage maybe excluded from further analysis. The process should include all risks, whether or not they are under the control of the Institution.

Risk identification : Steps to Identify Risks

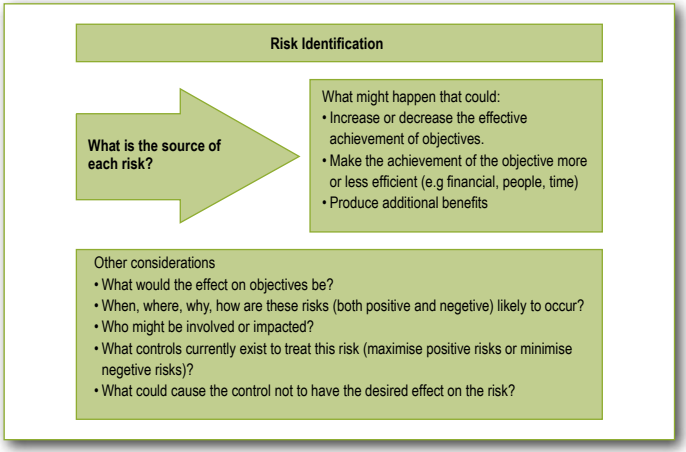
It is important that the risk identification exercise does not get bogged down in conceptual or theoretical detail. It should also not limit itself to a fixed list of risk categories, although such a list may be helpful.

THESE STEPS ARE DISCUSSED IN-DETAIL BELOW:

a. Understand what to consider

In order to develop a comprehensive list of risks, a systematic process should be used that starts with the defining objectives and key success criteria for their achievement. This can help provide confidence that the process of risk identification is complete and major issues have not been missed.

Figure 2: Risk Identification - questions about each of the key elements



b. Gather information to identify risks

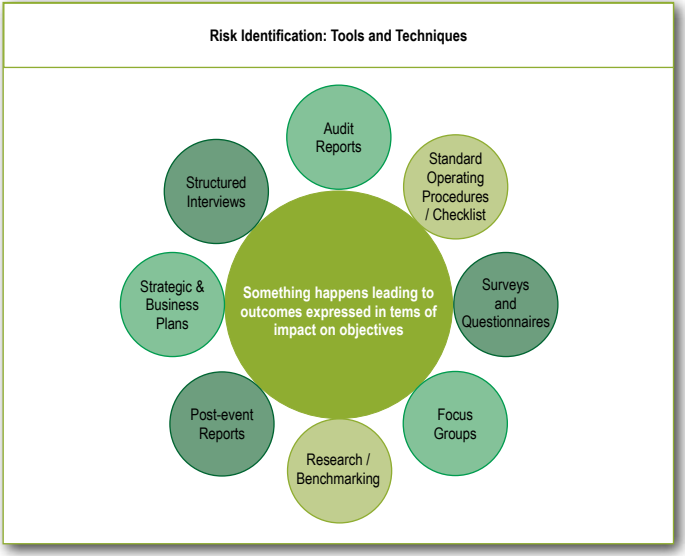
Good quality information is important in identifying risks, it is also crucial to have knowledge of the business before commencing with the identification process. The starting point for risk identification may be historical information about this or similar institutions and then discussions with a wide range of stakeholders about historical, current and evolving issues, data analysis, review of performance indicators, economic information, loss data, scenario planning and the like can produce important risk information.

Furthermore, processes used during strategic planning like SWOT Analysis, PEST(EL) Analysis and benchmarking will have revealed important risks and opportunities that must not be ignored i.e. they must be included.

c. Apply risk identification tools

Institutions should apply a set of risk identification tools and techniques that are suited to its objectives and capabilities, and to the risk the organisation faces. Relevant and up-to-date information is important in identifying risks. This should include suitable background information where possible. People with appropriate knowledge should be involved in identifying risks.

Figure 3: Risk Identification: Tools and Techniques



- Approaches used to identify risks could include the use of checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis, and system engineering techniques.

- The approach used will depend on the nature of the activities under review, types of risks, the organisational context, and the purpose of the risk management exercise.
- Team-based brainstorming for example, where facilitated workshops is a preferred approach as it encourages commitment, considers different perspectives and incorporates differing experiences.
- Structured techniques such as flow charting, system design review, systems analysis, Hazard and Operability (HAZOP) studies and operational modelling should be used where the potential consequences are catastrophic and the use of such intensive techniques are cost effective.
- Since risk workshops are useful only for filtering and screening of possible risks, it is important that the workshops are supplemented by more sophisticated or structured techniques described above.
- For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure, such as 'what-if' and scenario analysis could be used.
- Where resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcomes within budget limitations. For example, where less time is available, a smaller number of key elements may be considered at a higher level, or a checklist may be used.

d. Document/ Record the risks identified

The risks identified during the risk identification are typically documented in a risk register and at this stage in the risk assessment process, typically includes:

- risk title and description

- how and why the risk can happen (i.e. contributing factors and consequences)
- the existing internal controls that may reduce the likelihood or consequences of the risks.

It is critically important at this stage to understand the cause-effect relationships between a risk, its causes, and the potential consequences should the risk occur. If the "wrong" risk is identified at this stage (e.g. causes or consequences, rather than the actual risk itself), it will reduce the value of the rest of the risk management process.

It is essential when describing a risk to consider the following three elements:

- description/event - an occurrence or a particular set of circumstances
- contributing factors – are causes that may contribute to a risk occurring or increase the likelihood of a risk occurring
- consequences - the outcome(s) or impact(s) of an event.

It is the combination of these elements that make up a risk and this level of detail will enable the DEAto better understand and manage the risk.

As a minimum, the risk register records:

- the risk
- how and why the risk can happen - "cause of risk"
- how will the risk impact the institution if it materializes "Impact on institution"
- the existing internal controls that may minimise the likelihood of the risk occurring
- the likelihood and consequences of the risk to the institution,
- a risk level rating based on pre-established criteria
- framework, including an assessment of whether the risk is

acceptable or whether it needs to be treated

- a clear prioritisation of risks (risk profile)
- accountability for risk treatment (may be part of the risk treatment plan)
- timeframe for risk treatment.

Once the risks have been identified and existing control have been assessed and it has been established that controls are inadequate, an assessment of whether the risk is acceptable or whether it needs to be treated needs to be performed.

Risk identification examples:

One can see from the following examples that failure to correctly define your risk will affect control identification, mitigation plan and ultimately reporting. Its the old "garbage in garbage out" analogy.

Tables 1 and 2 provide some examples of "good" and "poor" risk descriptions, adapted from AUS/NZ Standard 2004.

Table 1: Examples of good risk descriptions

Example 1: Good Risk Description	
Risk Description	High employee turnover
Contributing Factors	Job dissatisfaction Uncompetitive remuneration
Impacts	Loss of corporate knowledge Delay in delivery of business objectives
Example 2: Good Risk Description	
Risk Description	Breach of OH&S Act
Contributing Factors	Lack of knowledge of legislative requirements No compliance program or register
Example 2: Good Risk Description	

Impacts	Adverse publicity Fines / penalties
Example 3: Good Risk Description	
Risk Description	IT Failure
Contributing Factors	Power outage Software failure
Impacts	Loss of data Business disruption

Table 2: Examples of poor risk descriptions

Example 1: Poor Risk Description	
Risk Description	Lack of succession planning.
Contributing Factors	Lack of handover time Reluctance to handover information
Impacts	Financial Business
Explanation: Lack of succession planning is a lack of a control.	
Example 2: Poor Risk Description	
Risk Description	Fines
Contributing Factors	Lack of knowledge of legislative requirements No compliance program or register
Impacts	Adverse publicity Fines / penalties
Explanation: Fines are really the impact to the organisation. In addition, the reason for identifying the cause is so that one can identify the right controls. This description is so wide that a control is difficult to define, other than “put in place a full compliance program”.	
Example 3: Poor Risk Description	
Risk Description	System not backed up.
Contributing Factors	IT failure
Impacts	Loss of data
Explanation: System not backed up is a control failure. Also an IT failure is not the cause of the system not being backed up, poor work practices are.	

3. DOCUMENT THE RISK IDENTIFICATION PROCESS

In addition to documenting the risks identified, it is also necessary to document the risk identification to help guide future risk identification exercises and to ensure good practices are maintained by drawing on lessons learned through previous exercises. Documentation of this step should include:

- the approach or method used for identifying risks,
- the scope covered by the identification,
- the participants in the risk identification and the information sources consulted.

Experience has shown that management often disregards well controlled risks when documenting the risk profile of the institution. It however must be stressed that a well-controlled risk must still be recorded in the risk profile of the institution. The reason for this logic is that the processes for identifying risks must ignore at that point any mitigating factors (these will be considered when the risk is being assessed)

4. THE OUTPUTS OF RISK IDENTIFICATION

The document in which the risks are recorded is known as the "risk register" and it is the main output of a risk identification exercise.

A risk register is a comprehensive record of all risks across the institution or project depending on the purpose/context of the register. There is no single blueprint for the format of a risk register and institutions have a great degree of flexibility regarding how they lay out their documents.

The risk register serves three main purposes

- The first is that it is a source of information to report the key risks throughout the institution, as well as to key stakeholders.

- The second purpose of the risk register is for the benefit of management. Management uses the risk register to focus their priorities.
- The third purpose of the risk register is to help the auditors to focus their plans on the institution's top risks.

GUIDEBOOK: CONTROL ACTIVITIES

1. INTRODUCTION

The institution can respond to risk through various mechanisms such as avoidance, transfer, accepting and managing of the risk. When the institution elects to manage the risk, it will require control activities to support the management of the risk to within tolerable levels.

2. OUTPUTS

Control activities will produce detailed action plans for managing all material risks.

3. CONTROL TYPES AND CONTROL TIMING

The risk assessment will have produced management's perspective of the effectiveness of the existing controls. This would inform management of additional control interventions required to better manage the risk exposures to an acceptable level. Management will be able to consider the best control options from various alternative control types:

a) Management controls

These ensure that the institutions structure and systems support its policies, plans and objectives and operate within laws and regulations;

b) Administrative controls

These ensure that policies and objectives are delivered in an efficient and effective manner and that losses are minimised;

c) Accounting controls

these ensure that resources allocated are accounted for fully and transparently and are properly documented;

d) Information technology controls

These controls relate to IT systems and include access control, controls of system software programmes, business continuity controls and other controls.

Each control type above can be further classified in terms of its timing as either:

i) Preventative controls

These are control measures that prevent a loss event from occurring, for example, segregation of duties in order to prevent fraud and errors by employees. These controls mitigate the probability of a risk.

ii) Detective controls

These are control measures that ensure that a loss event is identified as soon as it occurs, in order to control the effect on the organisation and to put preventative controls in place to prevent a re-occurrence. These controls mitigate the impact of a risk.

iii) Contingent controls

A control measure that is dependent on the happening of an event; and is also known as a corrective control. The control will minimise the impact of the event occurring, e.g. insuring an insurable event. Contingent controls, by their nature will be more effective for risks with a low probability of occurrence but which have a severe impact, e.g. insure fixed property against loss by fire.

4. CONSIDERATIONS FOR IMPROVING CONTROLS

The following questions could provide useful information for a high level understanding of the underlying issues and the control improvements required:

a) What is the risk assessment telling us about the effectiveness of the current controls (What needs to be enhanced)?

b) What are the various options available for addressing the residual risk?

c)What amount and quality of information do we have about the risk (what additional information is required to fully understand and respond to this risk)?

d)How much is the additional control going to cost and how does this compare with the benefits to be derived from the additional control?

e) Is there a necessity for introducing new policies and procedures, or updating the existing policies and procedures?

f) How will we measure whether the new control measures are working or not?

g) What is the action plan for addressing the control gaps?

h) Who is the responsible person?

i) What project plans should we put in place?

5. ASSURANCE ON CONTROL ACTIVITIES

Up until now the control adequacy and effectiveness was based exclusively on management perception. The inherent danger in this is that "optimism bias" could prevail, that is to say, management is more optimistic about the control environment than they really should be.

An examination of the control activities performed by an independent party has the advantage of eliminating "optimism bias" and revealing a more realistic perspective of the control activities.

Independent assurance can be provided by internal audit, a corporate function, independentconsultants or the Auditor-General.

The reports provided by these assurance providers should be utilised to update the assessments reflected in the risk register and should form the basis for developing additional control enhancements that is required.

GUIDEBOOK: RISK ASSESSMENT

1. INTRODUCTION

The risk assessment is a systematic process to understand the nature of risk and determine the level of risk. The risk assessment step aims to develop an understanding of the risk. It provides an input to decisions on whether risk response is necessary and the most appropriate and cost-effective risk response strategies.

The main purpose of risk assessment is to help management to prioritise the identified risks. This enables management to spend more time, effort and resources to manage risks of higher priority than risks with a lower priority.

Risk assessment is a fundamental component of the risk management process. It helps to guide the evaluation of risks by defining the key parameters of the risk and how these may impact on the achievement of institution's objectives.

One of the key outcomes of the risk assessment process is determining levels of risk exposure for the institution. In addition, the data and related information collected during the risk assessment process can be used to assist in guiding risk response decisions.

2. THE APPROACH

Risk assessment involves interrogating risks at two levels, namely at the inherent risk level and the residual risk level, using the same rating criteria for each assessment.

- Inherent Risk: considers the "worst case" scenario. This involves considering the likelihood (frequency of risk occurrence) and impact (Outcome or consequence of an event) of the risk in the absence of any management control interventions. This level of assessment provides a perspective of the consequences of the risk to the institution in its unmanaged state.
- Residual risk: is the level of risk remaining after the mitigating influence of the existing control interventions is considered. Normally, management would introduce sufficient control to reduce the risk to within a pre-determined level, as informed by the risk appetite. The residual risk is a critical indicator of whether the existing controls are effective in reducing the risk to an acceptable level.

Risks can be assessed on a quantitative basis or a qualitative basis. Quantitative assessment works best for risks that involve numeric functions. A good example would be the risk of financial losses as this can be numerically quantified.

Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities.

Qualitative assessment is applied when the risk in question does not lend itself to numeric quantification. In such cases more subjective means are utilised, the most important of which is the expert judgement of management.

Risk assessment involves the following key steps:

a) Identify and evaluate existing control effectiveness

b) Determine risk likelihood (frequency of risk occurrence) and risk impact (outcome or consequence of an event)

c) Both the risk likelihood and impact rating should be performed prior and post controls to determine level of risk rating (Inherent vs. residual rating).

d) Determine risk rating level

These steps are discussed in-detail below:

a) Identify and evaluate control effectiveness

Controls may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. Residual risk will therefore inform management of the actual level of control effectiveness.

Controls should be considered on the basis of:

- design effectiveness - is the control "fit for purpose" in theory i.e. is the control designed appropriately for the function for which it is intended

- operational effectiveness - does the control work as practically intended. It is useful to involve staff with an understanding of the controls when rating them. Internal audit, business analysts and operational/ financial management can all provide input into control identification and assessment.

A well-designed and implemented control can often mitigate or reduce more than one risk or type of risk.

b) Determine the risk impact and likelihood

Risks are assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence. (Risk = Likelihood x Impact)

The magnitude of the consequences of an event, should it occur, and the likelihood of the event and its associated consequences, should be assessed in the context of the effectiveness of the existing strategies and controls.

Consequences and likelihood may be estimated using statistical assessment and calculations. Where no reliable or relevant past data is available, subjective estimates may be made which reflect an individual's or institution's degree of belief that a particular event or outcome will occur.

The most relevant sources of information and techniques should be used when analysing consequences and likelihood.

Sources of information

i) Past records;

ii) Practice and relevant experience;

iii) Relevant published literature;

iv) Research;

v) The results of public consultation;

vi) Experiments and prototypes;

vii) Specialist and expert judgments.

Techniques:

i) Structured interviews with experts in the area of interest;

ii) Use of multi-disciplinary groups of experts;

iii) Individual evaluations using questionnaires;

iv) Use of models and simulations.

Risk assessment should be performed in accordance with approved rating criteria for both likelihood and impact (Refer to Guidebook Risk Rating).

c) Determine the overall risk rating

Once you have rated the likelihood and consequence, combine the two to determine the overall risk rating.Based on the risk assessment, risks are classified by level to determine the appropriate level of response to those risks. Specific responses are defined at the "Risk Response" phase (Refer to Guidebooks Risk Rating and Risk Response Strategy)

d) Document the risk assessment process

Documentation of the risk assessment process provides a record of how risks were analyzed in previous periods, thereby informing future risk assessment exercises. A key outcome of documenting the risk assessment process is enabling accurate tracking of risks over time using historical reference data.

Documentation should include:

i) key assumptions and limitations

ii) sources of information used

iii) explanation of the assessment method, and the definitions of the terms used to specify the likelihood and consequences of each risk

iv) existing controls and their effectiveness
v) description and severity of consequences
vi) the likelihood of these specific occurrences
vii) resulting level of risk

Detailed documentation may not be required for very low risks; however a record should be kept of the rationale for initial screening of very low risks.

e) The outputs of the risk assessment process

The output of risk assessment is a more sophisticated risk register which is enriched by the addition of ratings for each risk. This allows management to separate the more important risks from the less important ones and direct management attention accordingly.

GUIDEBOOK: RISK RATING

1. IMPACT

The DEA a five-point rating scale to assess the potential impact of risks, with 1 being the lowest impact and 5 being the highest impact.The following is the rating table used by the DEA.

Table 3: Impact rating table

Severity Ranking	Continuity of Service Delivery	Safety & Environ-mental	Technical Complexity	Financial
Critical 5	Risk event will result in widespread and lengthy reduction in continuity of service delivery to customers for a period greater than 48 hours	Major environmental damage. Serious injury (permanent disability) or death of personnel or members of the Public.Major negative media coverage.	Use of unproven technology for critical systems /project components. High level of technical interdependencies between system components.	Can lead to termination of Business activity
Major 4	Reduction in service delivery or disruption for a period ranging between 24 & 48 hours over a significant area	Significant injury of personnel or public. Significant environmental damage. Significant negative media coverage.	Use of new technology notpreviously utilised by the organisation for critical systems / project components.	Cost increase > 10%
Moderate 3	Reduction in service delivery or disruption for a period between 8 & 24 hours over a significant area	Lower level of environmental, safety or health impacts. Negative media coverage	Use of unproven or emerging technology for critical systems / project components.	Cost increase > 5%
Minor 2	Brief local inconvenience (work around possible). Loss of an asset with minor impact on operations	Little environmental, safety or health impacts. Limited negative media coverage.	Use of unproven or emerging technology for systems / project components.	Cost increase < 1%

Severity Ranking	Continuity of Service Delivery	Safety & Environ-mental	Technical Complexity	Financial
significant 1	No or minimal impact on business or core systems	No environmental, safety or health impacts and/or negative media coverage	Use of unproven or emerging technology for non-critical systems / project components	Minimal or no impact on cost

2. LIKELIHOOD

The DEA a five-point rating scale to assess the likelihood of risks, with 1 being the lowest likelihood and 5 being the highest likelihood. The following is the rating table used by the DEA.

Table 4: Likelihood rating table

Probability Factor	Measurement Criteria	Qualification Criteria	Rating
Common	The risk is already occurring, or has a high likelihood of occurring more than once during the next 12 months	The risk is almost certain to occur in the current circumstances	**5**
Likely	The risk will easily occur, and is likely to occur at least once during the next 12 months	More than an even chance of occurring	**4**
Moderate	There is an above average chance of the risk occurring more than once during the next 3 years	Could occur often	**3**

Probability Factor	Measurement Criteria	Qualification Criteria	Rating
Unlikely	The risk has a low likelihood of occurring during the next 3 years	Low likelihood, but could happen	**2**
Rare	The risk is unlikely to occur during the next 3 years	Not expected to happen - event would be a surprise	**1**

3. RISK EXPOSURE (IMPACT X LIKELIHOOD)

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

Table 5: Risk exposure

Risk Rating	Assessment	Definition
20 - 25	**Extreme**	Extremely unacceptable level of residual risk – implies that there are no controls in place or controls are completely ineffective. Risk must be escalated to the DDG/DG/DM/MINISTER.
>= 10 to < 20	**High**	Unacceptable level of residual risk - Implies that the controls are either fundamentally inadequate (poor design) or ineffective (poor implementation).
> 5 to < 10	**Medium**	Cautionary level of residual risk - Implies that the controls are either inadequate (poor design) or ineffective (poor implementation).
>= 5	**Low**	Mostly acceptable level of residual risk – managed at operational level using current controls.

GUIDEBOOK: RISK RESPONSE STRATEGY

1. INTRODUCTION

A key outcome of the risk identification and evaluation process is a detailed list of all key risks including those that require treatment as determined by the overall level of the risk against the DEA's risk tolerance levels. However, not all risks will require treatment as some may be accepted and only require occasional monitoring throughout the period.

All key risk identified should be responded to however not all of these risks will require treatment. The risks that fall outside of the DEA' s risk tolerance levels are those which pose a significant potential impact on the ability of the DEA to achieve set objectives and therefore require treatment.

The purpose of responding and treating risks is to minimize or eliminate the potential impact the risk may pose to the achievement of set objectives.

Risk response involves identifying the range of options for responding to risks, assessing these options and the preparation and implementation of response plans.

Risk response may involve a cyclical process of assessing a risk response, deciding that current risk levels are not tolerable, generating new risk response/s, and assessing the effect of that response until a level of risk based on the agreed risk criteria is reached.

2. DEVELOPING A RISK RESPONSE STRATEGY

Risk response plans identify responsibilities, schedules, the expected outcome of responses, budgets, performance measures and the review process to be set in place.

The risk response plan usually provides detail on:

i) actions to be taken and the risks they address;

ii) who has responsibility for implementing the plan;

iii) what resources are to be utilized;

iv) the budget allocation;

v) the timetable for implementation;

vi) details of the mechanism and frequency of review of the status of the response plan.

How to respond to risks?

Responding to risks involves the following key steps, each of which is covered in detail in this section:

a) Identify risk response and select risk response options

b) Assign risk ownership

c) Prepare risk response plans

d) Identify risk response options.

These steps are discussed in detail as follows:

a) Identify and select appropriate risk response option

Risk response design should be based on a comprehensive understanding of how risks arise. This includes understanding not only the immediate causes of an event but also the underlying factors that influence whether the proposed response will be effective. Once risks have been assessed and a level of risk rating has been assigned, an option for response is selected. It must be noted, that risk response options are not necessarily mutually exclusive or ap-

propriate in all circumstances. Table 6, details the risk response options adopted by the DEA.

Table 6: Risk response options

Risk response	Definition
Avoid	Steps taken to prevent the occurrence of hazards, such as: ceasing activity or changing objective.
Mitigate	Steps taken to reduce either the likelihood of an occurrence or impact or both.
Transfer	Steps taken to shift loss or liability to third parties, such as: insurance or outsourcing.
Accept	Informed decision to accept both the impact and likelihood of risk events.

Consideration should be given to the cost of the response option as compared to the likely risk reduction that will result.For example, if the only available response option would cost in excess of R10M to implement and the cost impact of the risk is only R5M, it may not be advisable.In order to understand the costs and benefits associated with each risk response option, it is necessary to conduct a cost-benefit analysis.

The steps for a basic cost benefits analysis are:

- Define, or breakdown the risk into its elements by drawing up a flowchart or list of inputs, outputs, activities and events.
- Calculate, research or estimate the cost and benefit associated with each element. (Include if possible direct, indirect, financial and social costs and benefits).
- Compare the sum of the costs with the sum of the benefits.

Prioritisation of risk response

The implementation of selected response strategies need to be prioritised base on the level of residual risk with reference to table 7.

Table 7: Prioritisation of risk response

Risk Level	Action priority	Action Timescale	Review Timescale
Extreme	Extremely unacceptable risk. Take immediate further action to reduce the risk; Contingency plan on standby.	Immediate	Review at least Monthly
High	Unacceptable risk. Quickly implement further action(s) to reduce risk; continue existing controls; generate contingency plan.	Immediate	Review at least every 2 months
Medium	Cautionary level of residual risk. Take action(s) to reduce risk; continue controls; generate contingency plan.	Within two months	Review at least every 3 months
Low	Tolerate/Accept; No action. Continue with existing control measures if required.	N/A	Review at least every 6 months

b) Assign risk ownership

Risk owners nominated by executive management should assume responsibility for developing effective risk response plans. The risk owner should be a senior staff member or manager with sufficient technical knowledge about the risk and/or risk area for which a response is required.The risk owner may delegate responsibility (but not accountability) to his/her direct reports or consultants for detailed plan development and implementation.

Prepare risk response plans:
Once response options for individual risks have been selected, all response options should be consolidated into risk action plans and/or strategies.

As one risk response may impact on multiple risks, response actions for different risks need to be combined and compared so as to identify and resolve conflicts between plans and to reduce duplication of effort.

Response plans should:

- identify responsibilities, schedules, the expected outcome of responses, budgets, performance measures and the review process to be set in place include mechanisms for assessing and monitoring response effectiveness, within the context of individual responsibilities; and
- Institution's objectives, and processes for monitoring response plan progress against critical implementation milestones. This information should all arise from the response design process.
- Document how practically the chosen options will be implemented.

GLOSSARY

Audit: The systematic review and assessment of the level of compliance of an actual situation or system with a standard of performance.

Action Plan: The actions developed or taken after the risk assessment process to reduce the probability and/ or impact of the event

Consequence: Outcome or impact of an event

Contributing Factor: An event and or issue that may gives rise to a risk event materialising

Contingent Control: A control measure that is dependent on the happening of an event; and is also known as a corrective control. The control will minimise the impact of the event occurring, e.g. insuring an insurable event. Contingent controls, by their nature will be more effective for risks with a low probability of occurrence but which have a severe impact, e.g. insure fixed property against loss by fire.

Control: The means used to manage risk. In particular, a policy, procedure, device, system, communication or other action that acts to limit uncertainty in the achievement of business objectives and/or to ensure compliance with the law.

Control Adequacy: An assessment of whether all the controls linked to a risk are adequate enough to manage the risk.

Control Effectiveness: An assessment of controls individually to determine whether or not the control is effective in achieving the desired outcome.

Detective Controls: These are control measures that ensure that a loss event is identified as soon as it occurs, in order to control the effect on the organisation and to put preventative controls in place to prevent a re-occurrence. These controls mitigate the impact of a risk.

Enterprise Risk Management (ERM): A structured and consistent approach that aligns strategy, processes, people, technology and knowledge, with the purpose of evaluating and managing the uncertainties the organisation faces to create value

Inherent Risk: Inherent risk is the risk to an organisation in the ABSENCE of any controls management might have in place to alter either the risk's impact or probability.

Impact: The effect of the risk on the DEA. Impacts may include reputation damage, financial loss, legal impacts, to name a few. The degree of harm, injury, loss or potential gain.

Impact score: A measure of the degree of consequences that are most likely to occur associated with a risk issue. Those consequences could either negatively impact the DEA and its stakeholders or be the expected level of unrealised opportunity for gain that could be missed.

Issue: An event that is currently happening, that needs to be addressed by appropriate corrective and preventative actions.

Preventative Controls: These are control measures that prevent a loss event from occurring, for example, segregation of duties in order to prevent fraud and errors by employees. These controls mitigate the probability of a risk.

Probability: The chance of occurrence per action, operation or opportunity. Expressed as a number between 1 and 5, with no units and not time related.

Residual risk: The level of risk that remains after the existing (and claimed) controls that are in place and their effectiveness are taken into account. These controls may require verification by audit.

Residual Risk Heat Map: Provides a graphical representation of the organisation's risk profile, by displaying the relationship between the probability of a risk occurrence and the severity of the impact thereof, once controls are in place.

Risk: An uncertain event that, if it were to occur, would have an effect on achieving strategic objectives.

Risk Assessment: The collaborative and consultative workshop or interview process whereby risks are identified measured and analysed according to a set methodology.

Risk Management: The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects.

Risk Appetite: This is the amount of risk, an entity is willing to accept in pursuit of value. It reflects the organisation's risk management philosophy and in turn influences the organisation's culture and operating style.

Risk Ranking: A way of sorting risks or actions arising out of a risk assessment according to the relative magnitude of the risk.

Risk Rating: The numerical rating applied to a risk calculated as the compound of an impact factor, and a probability factor.

Risk Register: A collection of risk information that defines the risk profile of the organisation, business unit, project or activity.

Risk Response: Once the key risks have been identified and assessed management should consider how to manage them and implement controls

Terminate / Avoid: Diversify or avoid an activity that will give rise to the risk

Transfer / Share: Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common techniques include purchasing insurance products, engaging in hedging transactions, or outsourcing an activity.

Treat / Manage: Treating a risk means taking steps to reduce or eliminate the probability of it occurring, the impact on the organisation if it arises, or a combination of both in order to bring the risk to acceptable levels in line with the organisation's risk appetite.

Tolerate / Accept: Tolerating or accepting a risk means that the organisation is willing to live with the consequences of a risk materialising.

Notes

Notes

Notes

Notes

Notes

against corruption today

Anti-Fraud Corruption hotline:
0800 701 701

315 Pretorius Street
cnr Pretorius & Lillian Ngoyi Streets
Fedsure Forum Building
North Tower
Pretoria, 0001

Call Centre: 086 111 2468

Postal Address
Private Bag X447
Pretoria
0001

www.environment.gov.za