

THE EASTERN CAPE
DEPARTMENT OF EDUCATION



DEPARTMENTAL RISK MANAGEMENT POLICY AND FRAMEWORK

Effective: 2020/2021

A handwritten signature in black ink, appearing to be 'J. ...', located at the bottom left of the page.

2.)

A handwritten signature in black ink, appearing to be '...', located at the bottom right of the page.

TABLE OF CONTENTS

	Page
1. DEFINITION OF TERMS	2
2. FOREWORD	5
3. PURPOSE	7
4. BACKGROUND	8
5. SCOPE OF APPLICABILITY.....	9
6. POLICY AND FRAMEWORK DEVELOPMENT	10
7. RISK MANAGEMENT MATURITY	11
8. DEFINING RISK AND RISK MANAGEMENT	13
9. OBJECTIVE:	15
10. RISK MANAGEMENT IMPLEMENTATION APPROACH	16
12. FRAUD PREVENTION AND ANTI-CORRUPTION PLAN.....	32
13. ACCEPTANCE.....	33
14. RISK MANAGEMENT POLICY AND FRAMEWORK REVIEW:	34



3)



1. DEFINITION OF TERMS

Establishing a risk management common language at Eastern Cape Department of Education (“the ECDoE or the Department”) is inherent to the provision of an equal understanding of risk management and the process thereof by all within the Department.

The common language provides a platform of cohesion that will enable all officials within the Department when relating to risk management matters to speak a common language and understand the terms used without confusion. This Appendix lists various terms with appropriate definitions that are used at the Department. These terms can be adapted as the needs and focus of the business change.

Accountability - Accountability refers to the mechanisms for demonstrating how delegated authority has been exercised, and for calling to account those to whom authority has been delegated.

Accounting Officer - Is the Head of the Department. He\she is also being the ultimate Chief Risk Officer of the Department and is accountable for the Department’s overall governance of risk.

Audit Committee - The Audit Committee is an independent committee responsible for oversight of the Department’s control, governance and risk management, established in terms of section 77 of the Public Finance Management Act 1 of 1999 (“PFMA”).

Consequence – The outcome of an event expressed qualitatively or quantitatively, being a loss or gain to the Department.

Cost – The cost of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, goodwill, political and intangibles losses.

Event - An incident or situation, which occurs in a particular place during a particular interval of time.

Frequency - A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also Likelihood and Probability.

Hazard - A source of potential harm or a situation with a potential to cause loss.

Impact – The effect that a risk would have on the Department if the risk materialises.

Inherent risk – The risk to the Department, which arises by virtue of the nature of the business activity.

Likelihood - A qualitative description of probability or frequency of the risk if it materialises.

Loss - Any negative consequence, financial or otherwise.

Management - refers to the team of officials who support the Accounting Officer in the management of the Department’s activities. This includes the Deputy Directors-General, Chief Directors, Directors, and Deputy Directors.

Monitor - To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change, and ensure the required progress is maintained.



Residual risk - The remaining level of risk after risk treatment measures and/or controls have been taken and/or put in place.

Risk – An unwanted outcome, actual or potential, to the Department’s service delivery and other performance objectives, caused by the presence of risk factors.

Risk acceptance – Responding to risk where cost and strategy consideration rule out alternative strategies.

Risk analysis - A systematic use of available information to determine how often specified risks may occur and the magnitude of their consequences.

Risk appetite - The amount of residual risk the Department is willing to accept in pursuit of its mission and vision.

Risk assessment - A process of evaluating the magnitude of the risk; in terms of the likelihood of the risk occurring, as well as the impact the risk may have on objectives should it occur.

Risk avoidance – Responding to risk by an informed decision not to become involved in a risk situation; for example, choosing a different strategy or terminating the activity that produces risks.

Risk control - Part of integration of risk management activities which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimize adverse risks.

Risk Culture - Set of shared risk management attitudes, values and practices that characterise how the Department considers its day-to-day activities.

Risk exploitation – Responding to risk opportunities by implementing strategies to take advantage of the opportunities presented by such risk factors.

Risk evaluation - The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

Risk factor: Any threat or event which creates, or has a potential to create risk.

Risk financing - The methods applied to fund risk responses and the financial consequences of risk.

Risk identification - The process of systematically identifying all possible risks, which may impact negatively on the Department.

Risk management - The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects, through a systematic and formalised process to identify, assess, manage and monitor risks.

Risk Management Committee – an oversight advisory body charged with the responsibility of discharging its governance responsibilities relating to risk management and anti-corruption activities.

Risk register – the formal documentation of the identification, assessment, management and the monitoring of risks.



2.



EASTERN CAPE DEPARTMENT OF EDUCATION
RISK MANAGEMENT POLICY AND FRAMEWORK

Risk retention - Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the Department.

Risk tolerance - The acceptable levels of variation relative to the achievement of objectives.

Risk transfer – Responding to risk, by shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

Risk treatment – responding to risks by implementing or improving on the internal control systems, selection and implementation of appropriate options for dealing with risk.

Sensitivity analysis - Examines how the results of a calculation or model vary as individual assumptions are changed.

Stakeholders - Those people and entities who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.

The ECD\Department – refers to the Eastern Cape Department of Education.



7.)



2. FOREWORD

As the ECDoE, we are committed to a process of risk management that is aligned to the principles of good corporate governance, as supported by the Public Finance Management Act (PMFA), Act 1 of 1999 as amended and various other pieces of legislations applicable to the ECDoE.

Risk management is recognised as an integral part of responsible management and the ECDoE therefore adopts a comprehensive approach to the management of risk. The features of this process are outlined in the Department's Risk Management Policy and Framework. It is expected that all programmes and/ or sections must work together in a consistent and integrated manner, with an overall objective of reducing risk to be within an acceptable level, as far as reasonably practical.

Effective risk management is imperative to the ECDoE to fulfil its mandate, the service delivery expectations of the public and the performance expectations within the Department. The realisation of our Strategic objectives depends on all employees being able to take calculated risks in a way that does not jeopardise the interest of stakeholders. Sound management of risk must enable the ECDoE to anticipate and respond to changes in its environment, as well as taking informed decisions under conditions of uncertainties.

The departmental staff must adhere to the fundamental principles that all resources must be applied economically to ensure:

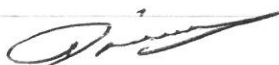
- The highest standards of service delivery;
- A management system containing the appropriate elements aimed at minimising risks and costs in the interests of all stakeholders;
- Maintaining an environment, which promotes the right attitude and sensitivity towards internal and external stakeholders' satisfaction;
- Educating and training of all staff to ensure continuous improvement in knowledge, skills and capabilities, which facilitate consistent conformance to the stakeholders' expectations.

No organisation operates in a risk-free environment, and no risk management process can guarantee such an environment. Risk management assists organisations to:

- Avoid certain adverse outcomes through taking proactive steps (fraud risk prevention, etc.)
- Help institutions cope when actual incidents do occur (disaster recovery plan, business continuity plan, etc.)
- Identify opportunities for continuous improvement.

Through the above, effective risk management therefore assists institutions to achieve their performance and service delivery targets, and to reduce the potential loss of resources. This results in effective responsibility and accountability structures, the improvement of the format used to report performance, and compliance with laws and regulations, thus avoiding damage to its reputation and other consequences. Additional key benefits include:

- Increasing probability of achieving objectives;
- Aligning risk appetite and strategy;
- Enhancing risk response decisions;
- Reducing operational surprises and losses;
- Identifying and managing multiple and cross-enterprise risks;
- Seizing opportunities;
- Ensuring proper financial and asset management;
- Better quality data for decision making;
- Resource deployment to deliver on planned targets;



EASTERN CAPE DEPARTMENT OF EDUCATION
RISK MANAGEMENT POLICY AND FRAMEWORK

As can be seen from the above, by being proactive and energetic in the embedding of the risk management process, there are many benefits to the institution.



?)



3. PURPOSE

This document is intended to guide the implementation of the Department's risk management policy and framework, so that a risk management culture is instilled in the Department. The document also outlines how the Department plans to effectively manage risks within the Department, and to improve the risk management maturity of the Department.

It also clarifies the various risk management roles and responsibilities, and the risk management reporting lines within the Department.

Risk management in the Department is concerned with managing threats and opportunities that it faces, and creating an environment of *'No Surprises.'*

By managing the Department's risks effectively, the Department will be in a stronger position to deliver our business objectives. By managing our opportunities well, we will be in a better position to provide improved services and better value for money.

This Risk Management Policy and Framework describes the processes that the Department has put in place and links together to identify, assess, manage, monitor and report on the risks; and describes the principles that underpin our approach. This document also points to other relevant sources of information where more guidance is available.



7.7



4. BACKGROUND

- I. The Department is bound by its constitutional mandate to provide services or goods in the interests of the public good.
- II. No institution has the luxury of functioning in a risk-free environment and public institutions, like ECDoE, are especially vulnerable to risks associated with fulfilling their mandate.
- III. The public sector environment is fraught with unique challenges such as inadequate capacity, excessive bureaucracy and silo mentality, limited resources, competing priorities and infrastructure backlogs to mention a few.
- IV. Such dynamics increase the risk profile of the public sector as a whole and place an extra duty of care on public sector managers to contain risks within acceptable limits.
- V. Risk management is a management tool which increases the institution's prospects of success through minimising negative outcomes and optimising opportunities.
- VI. Local and international trends confirm that risk management is a strategic imperative rather than an option within high performance organisations.
- VII. High performing organisations set clear and realistic objectives, develop appropriate strategies aligned to the objectives, understand the intrinsic risks associated therewith and direct resources towards managing such risks on the basis of cost-benefit principles.
- VIII. The Department must, in accordance with the prescripts mentioned below, implement and maintain effective, efficient and transparent systems of risk management and internal control.
- IX. The underlying intention of VIII above is that the Department must through risk management processes achieve, amongst others, the following outcomes needed to underpin and enhance performance:
 - More sustainable and reliable delivery of services;
 - Informed decisions underpinned by appropriate rigour and analysis;
 - Innovation;
 - Reduced waste;
 - Prevention of fraud and corruption;
 - Better value for money through more efficient use of resources; and
 - Better outputs and outcomes through improved project and programme management.



7-1



5. SCOPE OF APPLICABILITY

This document presents the Department's Risk Management Policy and Framework on risk management. The Risk Management Policy and Framework is facilitated by the Risk Management (RM) Function and reviewed by the Risk Management Committee structure, and thereafter approved by the Accounting Officer.



7.)



6. POLICY AND FRAMEWORK DEVELOPMENT

Development of this Policy and Framework has taken into account much of the latest research done by the Committee of Sponsoring Organisations ("COSO"), the enterprise-wide risk management (EWRM), the King IV Report on Corporate Governance (King IV Report) and the Public Sector Risk Management Framework ("PSRMF"). The framework consequently views risk management in relation to objective setting, risk identification, risk assessment, risk response and control, communication and monitoring.



7. RISK MANAGEMENT MATURITY

The Department has adopted the National Treasury's Risk Management Maturity Model ("RM Maturity") in order to measure its level of maturity with regard to risk management. This assists the Department in registering its risk management maturity improvement. The RM Maturity is made up of six levels, summarised as follows:

Level 1 – Non-existent :

- I. A public institution will be deemed to be in this level, if there is a lack of formalised risk management processes to deal with future uncertainties. No attempts are made to identify risks, and develop mitigation plans. The public institution, management and employees have an overall lack of awareness of risk management principle

Level 2 –

- II. Initial/Ad Hoc:

A public institution is deemed to have reached the initial or ad hoc level when the public institution has recognized the need for formal risk management processes. At this level risk management processes are repetitive and reactive, with little or no attempt to learn from past experiences or to prepare for future uncertainties. No attempt is made to identify risks or to develop mitigation or contingency plans. The normal method for dealing with risks is to react after risk eventuation with no proactive thought. During risk eventuation, operational processes are normally abandoned, downscaled, or temporarily abandoned and management hopes for the best. Occasionally, capable officials can identify and mitigate risks; but when they leave, their influence leaves with them. Even strong operations plans cannot overcome the instability created by the absence of sound risk management practices. At this level, some public institutions are experimenting with the application of risk management, usually through a limited number of individuals. At this level, public institutions would have no formal or structured risk management processes in place. Although the public institution is aware, at some level, of the potential benefits of managing their risks, there are no effectively implemented enterprise-wide processes.

Level 3 –

- III. Repeatable: Departmental-wide risk assessments have been completed and the necessary departmental capacity and structures to support risk management are in place. Risk management processes, practices and systems satisfy all legislative requirements at this stage but have limited influence on the control environment.

At the repeatable Level, a public institution would have implemented risk management into their routine processes. Risk management is implemented in most, if not all, units. Generic risk policies and procedures are formalized and the benefits of risk management are understood at all levels of the public institution. There is some risk management success stories in some programmes. Risk management capability is enhanced by establishing basic risk management disciplines on a routine basis. Programmes or units implement risk management through processes that are defined, documented, practiced, measured, enforced, and improvable. All units or programmes would typically have an identified risk owner. The basic requirement for achieving Level 3 is that there be policies that guide the units, or programmes in establishing the appropriate management processes. Capability of Level 3 can be summarized as disciplined because earlier successes can be repeated. The public institution's risk management processes are under the effective control of a defined system, following realistic plans based on the performance of previous experiences or bench marking on success stories.



7



Level 4 – Managed: A public institution would have attained the managed Level, when the public institution has established a risk-aware culture that utilizes a proactive approach to the management of risks in all aspects of the public institution. Appropriate information is continually developed and actively used to improve all the public institutions processes. Standard risk management processes are documented and utilized across the public institution. Risk management responsibilities have been assigned to individuals (risk owners, committees, coordinators, etc) in the public institution, thus opening formal and effective communication channels. Risk awareness interventions, training programs, etc are implemented to ensure that the officials have the required knowledge and skills to fulfill their assigned roles

IV. **Level 5 – Optimised :**

The optimized level is attained when public institution's establishes an institution-wide continuous improvement programme that takes into account lessons learned and best practices. Information Technology systems are utilized to achieve risk management objectives

The Department has developed a Risk Management Implementation Plan in order to ensure that the risk management process is driven to and matures to a compliance level (level 3) by the end of the 2019\2020 financial year. A Risk Management Improvement Plan (separate document) is developed annually to ensure that the Department has a consistent risk management improvement registered in terms of its risk management maturity, and ultimately maintenance of the highest level of risk management maturity in the Department.



2,



8. DEFINING RISK AND RISK MANAGEMENT

A risk can be defined as “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.”

Risks can be viewed from three distinct perspectives:

- Risk as an opportunity;
- Risk as an uncertainty; or
- Risk as a hazard.

Risk as an opportunity

Viewing risk from the opportunity perspective recognises the inherent relationship between risk and return. Managing risk as an opportunity necessitates actions being taken by business managers to achieve positive gains. Opportunity analysis creates insights that may be used by business managers to increase the likelihood of success and decrease the likelihood of failure.

Risk as an uncertainty

When considering risks from these perspective business units must determine how they can be proactive in preventing uncertain future events from having a negative impact. The management of uncertainty seeks to ensure that a business unit's actual performance falls within a defined range. The management of uncertainty risk is proactive. One must anticipate the impact of change and establish controls/processes designed to mitigate its effect on the operations of the business unit.

Risk as a Hazard

Risks may be viewed as the possibility of a negative event taking place or the fact that the negative event has taken place. Such potential negative events include financial loss, fraud, theft and damage to assets.

Types of Risks

Strategic Risks

Strategic risks are risks emanating from the strategic choices made by the Institution, specifically with regard to whether such choices weaken or strengthen the Institution's ability to execute its Constitutional mandate

Operational Risks

Operational risk are “risks concerned with the Institution’s operations” i.e. “operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events.”



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 management process is detailed under 10.1.



9. OBJECTIVE:

The objective of this policy and framework is to create a favourable risk management culture at all levels within the Department and to provide a strong commitment towards the following values:

- Reporting obligations;
- Sound financial and risk management practices;
- Strengthen values, ethics and protocols;
- Ensure a control environment on transparency and open government practices;
- Employees to be aware of risks and fraud risks;
- Provide sound, creative and client driven practices;
- Ensure a mature framework of delegation, rewards and sanctions;
- Achieve and improve a cultural change in government practices; and
- Consider all spheres of government practices and commitments and to improve risk transparency.

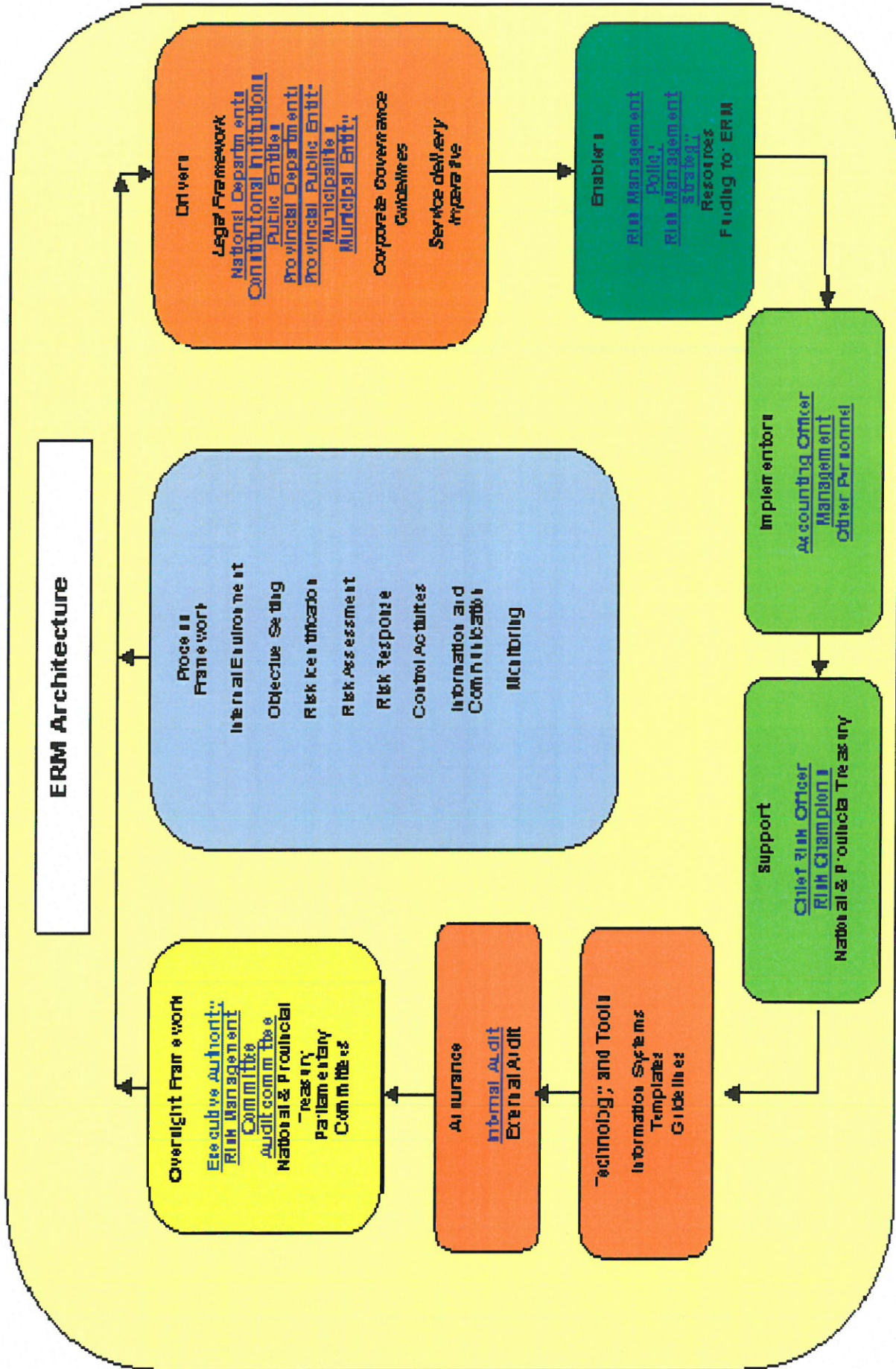


10. RISK MANAGEMENT IMPLEMENTATION APPROACH

The Department has adopted the risk management architecture that considers various interrelated and inter-dependent components of risk management in its attempt to implement a system of risk management.

- i. A process framework consisting of eight components guides the process of risk management within the Department.
- ii. Drivers that stabilise and govern risk management in the Department as far as legislation is concerned.
- iii. Enablers that translate the stance of risk management within the Department and also serve as guidance for instilling risk management into the Department.
- iv. Human resource capacity consisting of implementers, support specialists and assurance providers and oversight framework, to ensure that risk management is installed efficiently and effectively.
- v. Tools and technology to assist with the human resources in instilling efficient and effective risk management within the Department.





Handwritten signature and initials

10.1 Components of Risk Management Process Framework

10.1.1 Internal Environment

The Department needs to create an environment in which risk management can function efficiently and effectively. In doing so, it commits to and has a plan in place to change the current culture of the Department.

The Departments environment is the foundation of risk management, providing the underpinning culture, discipline and structures that influence how strategy and objectives are established and how Departmental activities are planned and executed and how risks are identified and acted upon.

10.1.2 Objective Setting

The Accounting Officer has set out the objectives of the Department, which are aligned to the Department's mandate. These objectives are the reference point of risk identification. These objectives include, amongst others; objectives from the Annual Performance Plan, objectives from short and long term projects, objectives from prioritised special intervention plans for the Departments and objectives for the Department's programmes, sub-programmes and all operations.

10.1.3 Risk Identification

Effective risk management begins with the question "what can go wrong?" that can prevent the Department from achieving its objective, and to ensure that risks are managed efficiently and effectively.

The approach that the Department is adopting in risk identification and documentation is objective, therefore, for every objective a risk identification and documentation process is performed by the responsible parties, facilitated by the Chief Risk Officer and/ or the dedicated risk management (RM) function.

Risk identification is broken down into three levels; strategic, operational and project risk identification.

The methods of risk identification that is used is dependent on the risk assessments to be conducted.

The risk identification process is as follows:

- I. The RM Function does preparatory work before conducting the risk identification. In doing this preparatory work, the RM Function considers (and does not limit itself to) the review of external and internal audit reports; review of the reports of the Standing Committee on Public Accounts and the relevant Parliamentary Committee(s); analysis of Executive Committee reports; financial analysis; historical data analysis; actual loss data; interrogation of trends in key performance indicators; benchmarking against peer groups or quasi peer group; market and sector information; scenario analyses; and forecasting and stress testing.
- II. Conduct the risk identification through risk management workshops or interviews by presenting the prepared work and leading and facilitating the risk identification process. The identification of risk is not limited to the internal environment; but the external environment is also considered.



2,



- III. The RM Function then documents all the risks identified into a risk register which is owned by the relevant managers.

10.1.4 Risk Assessment

An assessment of risk is done by the Departmental officials in their level of responsibilities facilitated by the RM Function. The risk assessment assists the Department in prioritising risks that have the highest threat to the Department.

Risks are assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence on the Department’s objective(s).

Risk assessment is performed through a two stage process:

- I. Firstly, the inherent risk is assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk, and
- II. Secondly, a residual risk assessment is performed to determine the actual remaining levels of risk after the mitigating effects of management actions to influence the risk.

Table 1 – Risk Rating Tables on Impact and Likelihood below guide the rating process on likelihood and impact, on both inherent and residual assessments.

Table 1 and 2 - Risk Rating Tables

Impact

The following rating table is utilised to assess the potential impact of risks.

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

Likelihood

The following rating table is utilised to assess the likelihood of risks.

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

The assessment of risks assists the Department in prioritising high risks that need an immediate response to, depending on the exposure of the risks. The exposure will be measured by multiplying the likelihood and the impact, and then categorised in three categories.

Table 3 – Inherent and Residual Risk Exposure (Impact X Likelihood) is an example of a rating table that can be utilised to categorise the various levels of inherent\residual risk.

Table 3 – Inherent\Residual Risk Exposure

RISK RATING	INHERENT OR RESIDUAL RISK MAGNITUDE	RESPONSE
15 - 25	High	Unacceptable level of risk - High level of control intervention required to achieve an acceptable level of residual risk
6 - 14	Medium	Unacceptable level of risk, except under unique circumstances or conditions - Moderate level of control intervention required to achieve an acceptable level of residual risk
1 - 5	Low	Mostly acceptable - Low level of control intervention required, if any

Risk map changed to eliminate the confusion that is caused when it comes to interpreting risk scores and reading of the risk maps. An example is indicated:

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

10.1.5 Risk Tolerance and Risk Appetite

The following key principles have underpinned our work on risk tolerance and risk appetite:

- I. Risk tolerance is the amount of uncertainty the Department is prepared to accept in total or more narrowly within a programme of a particular risk category or for a specific initiative.
- II. Risk appetite can be complex. Excessive simplicity, while superficially attractive, leads to dangerous waters: far better to acknowledge the complexity and deal with it, rather than ignoring it.
- III. Risk appetite needs to be measurable. Otherwise there is a risk that statements become empty and vacuous. We are not promoting any individual measurement approach but fundamentally it is important that directors should understand how their performance drivers are impacted by risk.
- IV. Our view is that both risk appetite and risk tolerance are inextricably linked to performance over time.

Risk Appetite	Risk Tolerance	
Acceptable Level (Low)	Medium	High
Qualitative Expression	Medium	High
Quantitative Expression	Medium	High
Business As Usual	Managing with intervention	Turnaround Strategy
Escalation Process	Accounting Officer	Minister

To provide guidance on the suggested response to risks falling into the indicated appetite and tolerance levels. Responses normally vary between tolerance, treatment, termination and transferring.

		RISK APPETITE LEVEL			RISK TOLERANCE THRESHOLDS		
No	Category	Acceptable 1- 5	Moderately Acceptable 6 - 14	Unacceptable 15 - 25	Low Risk 1 - 5	Medium Risk 6 - 14	High Risk 15 - 25
1	All	Treat Transfer Tolerate	Treat Transfer	Terminate Treat	Treat Transfer Tolerate	Treat Transfer	Terminate Treat

10.1.6 Risk Responses

Risk response is concerned with developing strategies to reduce or to eliminate the threats and events that create risks. All key risks identified are responded to; however, not all risks 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 is concerned with developing strategies to reduce or eliminate the threats and events that create risks. Risk response should also make provision for the exploitation of opportunities to improve the performance of the Department. Responding to risk involves identifying and evaluating the range of possible options to mitigate risks and implement the chosen option. Management

7,

should develop response strategies for all material risks, whether or not the management thereof is within the direct control of the Department, prioritising the high risks.

Where the management of the risk is within the control of the Department, the response strategies consider the following:

Terminate the risk by, for example, choosing a different strategy or terminating the activity that produces the risk;

- I. Treating the risk by, for example, implementing or improving the internal control system;
- II. Transferring the risk to another party more competent to manage it by, for example, contracting out services, establishing strategic partnerships and buying insurance;
- III. Tolerate the risk where cost and strategy considerations rule out alternative strategies; and,
- IV. Exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.

In instances where the management of risk is not within the control of the Department, the response strategies should consider measures such as forward planning and lobbying. Response strategies are documented and the responsibilities and timelines attached thereto are communicated to the relevant persons.

10.1.7 Control Activities

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

The risk assessment produces a management's perspective of the effectiveness of the existing controls. This informs management of additional control interventions required to better manage the risk exposures to an acceptable level. Management then is able to consider the best control options from various alternative control types:

- I. **Management controls** - these ensure that the Department's structure and systems support its policies, plans and objectives and operate within laws and regulations;
- II. **Administrative controls** - these ensure that policies and objectives are delivered in an efficient and effective manner and that losses are minimised;
- III. **Accounting controls** - these ensure that resources allocated are accounted for fully and transparently and are properly documented;
- IV. **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 classified as either:

- I. **Preventative controls** – these controls are designed to discourage errors or irregularities from occurring e.g. adequate physical security of assets to prevent losses such as theft or damage. If properly enforced, these controls are usually the most effective type of controls;
- II. **Detective controls** – these controls are designed to find errors or irregularities after they have occurred e.g. performance of reconciliation procedures to identify errors;
- III. **Corrective controls** – these controls usually operate together with detective controls in order to correct identified errors or irregularities.



2



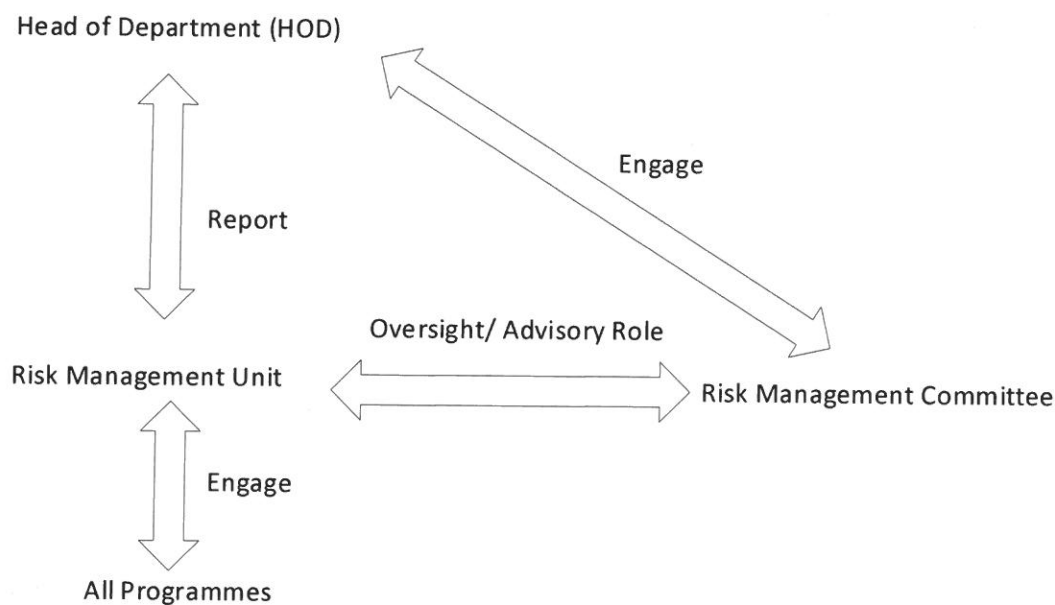
10.1.8 Communication and Reporting

The Department has a need to define and communicate risk reporting arrangements to all its stakeholders.

Common language, consistent form of reporting and collaboration among stakeholders (Committees, Management, Chief Risk Officer, etc) are critical to ensuring that risk reports are effectively utilised to drive departmental performance. It is also crucial that risk reporting is not only a bottom up approach. While risk reporting is meant to aid Managers to make risk-based decisions, it is equally important for such information and decisions to be communicated to operational staff and/or relevant officials in the Department.

Each individual within the Department gets a risk register to communicate risk information for her/his area of responsibility. The register is monitored by the immediate supervisor and the Risk Management Function. Various supervisors update programme heads on risk information on a monthly basis. Risk information gets reported at top management meetings at head office and at Cluster fincom meeting quarterly.

Table 4 – Risk management information reporting structure is adopted by the Department in reporting its risk management information.



10.1.9 Monitoring

A critical aspect that needs attention in order to create such an environment is the cultural change within the Department.

Monitoring is effected through on going activities to ascertain whether risk management is effectively practised at all levels and across the Department in accordance with the risk management policy, strategy and plan.

Drivers of Risk Management

The implementation of risk management within the Department is driven by the relevant framework. The application risk management legal framework relevant for the Department is as follows:

- I. Section 38 (1) (a) (i) of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA) requires that: *“The accounting officer has and maintains an effective, efficient and transparent systems of financial and risk management and internal control.”*
- II. Section 3.2.1 of the Treasury Regulations: The roles and responsibilities for the implementation of the ERM strategy are contained in the Treasury Regulations published in terms of the PFMA. Section 3.2.1 of the regulations addresses risk management and summarised as follows:
 - a. The accounting officer must ensure that a risk assessment is conducted regularly to identify emerging risks for the institution.
 - b. 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.
 - c. The risk management strategy must be clearly communicated to all officials to ensure that it is incorporated into the language and culture of the institution and embedded in the behaviour and mind-set of its people.
- III. Section 45 of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA): The extension of general responsibilities in terms of Section 45 of the PFMA to all managers within the public sector implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officer and internal audit.
- IV. Section 3.2.7. (a) of the Treasury regulations states: *“An internal audit unit must prepare, in consultation with and for approval by the audit committee –*
 - a. *A rolling three-year strategic internal audit plan based on its assessment of key areas of risk for the institution, having regard to its current operations, those proposed in its strategic plan and its risk management strategy.”*
- V. Section 3.1.10 of the Treasury Regulations states:
 - a. *The effectiveness of the internal control system;*
 - b. *The effectiveness of internal audit;*
 - c. *The risk areas of the Department’s operations to be covered in the scope of the internal and external audits;*
 - d. *The adequacy, reliability and accuracy of financial information provided to management and other users of such information;*
 - e. *Any accounting and auditing concerns identified as a result of internal and external audits;*
 - f. *The entity’s compliance with legal and regulatory provisions; and*
 - g. *The activities of the internal audit function, including its annual work programme, co-ordination with external auditors, the reports of significant investigations and responses of management to specific recommendations.”*

10.2 Enablers of Risk Management

Risk management enablers like Risk Management Policy and Framework (this document) with a risk management implementation plan assist the Department in guiding the entrenchment of risk management within the Department.



To be fully effective, these documents should be adequately communicated throughout the Department.

10.3 Role players and responsibilities

10.3.1 Oversight

Provincial Treasury

The Provincial Treasury functions in accordance with the applicable legal framework: Amongst other responsibilities, the Provincial Treasury, in terms of its risk management responsibilities:

- I. Prescribes uniform risk management norms and standards;
- II. Monitors and assesses the Department's implementation of the PFMA;
- III. Assists the Department in building its capacity for efficient, effective and transparent risk management; and
- IV. Enforces the PFMA by enforcing legislation and any other prescribed norms and standards for risk management in the Department.

The Provincial Treasury plays dual roles in terms of risk management, as oversight and support for the Department.

Executive Authority (MEC)

The MEC takes interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the Department against significant risks.

In doing so, the Accounting Officer has the following risk management responsibilities:

- I. Ensures the identification and management of key inherent risk in the Department's strategic choices are done rigorously; and
- II. Assists the Accounting Officer to deal with fiscal, intergovernmental, political, and other risks beyond their direct control and influence.

Risk Management Committee

The Risk Management Committee (RMC) is appointed by the Accounting Officer to assist in discharging the Accounting Officer's responsibility for risk management.

The mandate of the RMC is guided by the RMC Charter approved by the Accounting Officer. In discharging its governance to risk management, the Risk Management Committee is accountable to the Accounting Officer within the Department.

The following are risk management responsibilities for the RMC:

- I. Review and recommend to the Accounting Officer all risk management related documentation;
- II. Review the Department's risk identification and assessment methodologies;
- III. Evaluate the extent of effectiveness of risk management within the Department;
- IV. Assess the implementation of the risk management policy and strategy (which is inclusive of a risk management plan);
- V. Review the material findings and recommendations by assurance providers on the system of risk management and monitor the implementation of such recommendation;
- VI. Develop its own key performance indicators for approval by the Accounting Officer;



- VII. Interact with the Audit Committee to share information relating to material risks of the Department; and
- VIII. Provide timely and useful reports to the Accounting Officer on the state of risk management together with the recommendations to address deficiencies identified.

Audit Committee

An Audit Committee is an independent committee responsible for oversight of the Department's control, governance and risk management.

The Audit Committee provides an independent and objective view on the Department's risk management effectiveness and evaluates the effectiveness of Internal Audit responsibilities in relation to risk management. The Audit committee must:

- I. Review and recommend disclosures on matters of risks in the Annual Financial Statements;
- II. Review and recommend disclosures on matters of risk and risk management in the Annual Report; and
- III. Provide regular feedback to the Accounting Officer on the adequacy and effectiveness of risk management in the Department, including recommendations for improvement;
- IV. Ensure that internal and external audit plans are aligned to the risk profile of the Department; and
- V. Satisfy itself that it has appropriately addressed the financial reporting risks, including risk of fraud; internal financial controls; and IT risks as they relate to financial reporting.

10.3.2 Support

Provincial Treasury

The Provincial Treasury functions in accordance with the applicable legal framework: Amongst other responsibilities, the Provincial Treasury, in terms of its risk management responsibilities:

- I. Prescribes uniform risk management norms and standards;
- II. Monitors and assesses the Department's implementation of the PFMA;
- III. Assists the Department in building its capacity for efficient, effective and transparent risk management; and
- IV. Enforces the PFMA by enforcing legislation and any other prescribed norms and standards for risk management in the Department.

The Provincial Treasury plays dual roles in terms of risk management, as oversight and support for the Department.

Chief Risk Officers

The primary responsibility of the Chief Risk Officer is to bring to bear his / her specialist expertise to assist the Department to embed risk management and leverage its benefits to enhance performance.

- I. Working with senior management to develop the Department's vision for risk management;
- II. Developing, in consultation with management, the Institution's Risk Management Policy and Framework incorporating, *inter alia*, the:
 - a. risk management policy and framework;
 - b. risk management implementation plan;
 - c. risk identification and assessment methodology;
- III. Communicating the risk management policy and framework to all stakeholders in the Department and monitoring its implementation;

- IV. Facilitating orientation and training for the Risk Management Committee;
- V. Training all stakeholders in their risk management functions;
- VI. Continuously driving risk management to higher levels of maturity;
- VII. Assisting Management with risk identification, assessment and development of response strategies;
- VIII. Monitoring the implementation of the response strategies;
- IX. Collating, aggregating, interpreting and analysing the results of risk assessments to extract risk intelligence;
- X. Reporting risk intelligence to the Accounting Officer, Management and the Risk Management Committee; and
- XI. Participating with Internal Audit, Management and Auditor-General in developing the combined assurance plan for the Department.

Risk Champion

The Risk Champion intervenes in instances where the risk management efforts are being hampered, for example, by lack of cooperation by management and other officials and the lack of institutional skills and expertise. The Risk Champion also adds value to the risk management process by providing guidance and support to manage "problematic" risks, and risks of a transversal nature that require a multiple participatory approach and involves:

- I. Intervening in instances where the risk management efforts are being hampered, for example, by the lack of co-operation by Management and other officials and the lack of departmental skills and expertise;
- II. Adding value to the risk management process by providing guidance and support to manage "problematic" risks and risks of a transversal nature that require a multiple participant approach; and
- III. The Risk Champion not assuming the role of the Risk Owner, instead assisting the Risk Owner to resolve problems.

10.3.3 Implementers

Accounting Officer

The Accounting Officer is ultimately accountable for the governance of risk in the Department. The Accounting Officer sets an appropriate tone by supporting and being seen to be supporting the Department's aspiration for risk management. High level risk management responsibilities of the Accounting Officer include:

- I. Setting an appropriate tone by supporting and being seen to be supporting the Department's aspirations for effective management of risks;
- II. Delegating responsibilities for risk management to Management and internal formations such as the Risk Management Committee Finance Committee, Information and Communication Technology Committee;
- III. Holding Management accountable for designing, implementing, monitoring and integrating risk management into their day-today activities;
- IV. Holding the internal structures referred to in (II.) accountable for performance in terms of their responsibilities for risk management;
- V. Providing leadership and guidance to enable Management and internal structures responsible for various aspects of risk management to properly perform their functions;
- VI. Ensuring that the control environment supports the effective functioning of risk management;
- VII. Approving the risk management policy, strategy, and implementation plan;



EASTERN CAPE DEPARTMENT OF EDUCATION
RISK MANAGEMENT POLICY AND FRAMEWORK

- VIII. Approving the fraud prevention policy, strategy and implementation plan;
- IX. Devoting personal attention to overseeing management of the significant risks;
- X. Leveraging the Audit Committee, Internal Audit, External Audit and Risk Management Committee for assurance on the effectiveness of risk management;
- XI. Ensuring appropriate action in respect of the recommendations of the Audit Committee, Internal Audit, External Audit and Risk Management Committee to improve risk management; and
- XII. Providing assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.

Management

Management is responsible for aligning the functional risk management methodologies and processes with the Departmental process, and overseeing the management of key risks in their areas of responsibilities. High level risk management responsibilities for management include:

- I. Executing their responsibilities as set out in the risk management strategy;
- II. Empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities, comprehensive orientation and on-going opportunities for skills development;
- III. Aligning the functional risk management methodologies and processes with the Departmental process devoting personal attention to overseeing the management of key risks within their area of responsibility;
- IV. Maintaining a co-operative relationship with the Risk Management Unit and Risk Champion;
- V. Providing risk management reports;
- VI. Presenting to the Risk Management and Audit Committees as requested;
- VII. Maintaining the proper functioning of the control environment within their area of responsibility;
- VIII. Monitoring risk management within their area of responsibility; and
- IX. Holding officials accountable for their specific risk management responsibilities.

Risk Co-ordinators

They are members of the staff with specific risk management support functions within a programme, sub-programme or unit. Their main risk management responsibility involves maintenance of functional risk register and assisting risk owners in ensuring adequate implementation of risk management processes and monitoring risk registers quarterly.

Monitoring activities should focus on evaluating whether:

- I. Allocated responsibilities are being executed effectively;
- II. Response strategies are producing the desired result of mitigating risks or exploiting opportunities; and
- III. A positive correlation exists between improvements in the system of risk management and Institutional performance.

Results of quarterly monitoring should be presented at quarterly directorate meetings. Minutes of these meetings and portfolio of evidence supporting implementation of response strategies should be maintained by all directorates.



7,



Personnel

Personnel are responsible for integrating risk management into their day-to-day activities. They ensure that their risk management responsibilities are executed and reported on. High level risk management responsibilities of other personnel include:

- I. Applying the risk management processes in their respective functions;
- II. Implementing the delegated action plans to address the identified risks;
- III. Informing their supervisors and/or the Risk Management Unit of new risks and significant changes in known risks; and
- IV. Co-operating with other role players in the risk management process and providing information as required.

10.3.4 Assurance

Internal Audit

The Internal Audit function provides an independent, objective assurance on the effectiveness of the Department's system of risk management. Furthermore, Internal Auditing should evaluate the effectiveness of the risk management system and provide recommendations for improvement where necessary. Other risk management responsibilities for Internal Audit include:

- I. Develop its internal audit plan on the basis of the key risk areas
- II. In terms of the International Standards for the Professional Practice of Internal Audit, determine whether risk management processes are effective is a judgment resulting from the Internal Auditor's assessment that:
 - a. Departmental objectives support and align with the Department's mission;
 - b. Significant risks are identified and assessed;
 - c. Risk responses are appropriate to limit risk to an acceptable level; and
 - d. Relevant risk information is captured and communicated in a timely manner to enable the Accounting Officer, Management, the Risk Management Committee and other officials to carry out their responsibilities.

External Audit

The External Audit provides an independent opinion on the effectiveness of risk management. In providing the opinion, the External Auditor usually focuses on:

- I. Determining whether the risk management policy, strategy and implementation plan are in place and are appropriate;
- II. Assessing the implementation of the risk management policy, strategy and implementation plan;
- III. Reviewing the risk identification process to determine if it is sufficiently robust to facilitate the timely, correct and complete identification of significant risks, including new and emerging risks;
- IV. Reviewing the risk assessment process to determine if it is sufficiently robust to facilitate timely and accurate risk rating and prioritisation; and
- V. Determining whether the management action plans to mitigate the key risks are appropriate, and are being effectively implemented.



7.)



10.4 Information

The Department makes reference of the Risk Management Policy and Framework (this document) and also has access to the Public Sector Risk Management Framework to use as a guideline to understanding risk management and the risk management process.



Handwritten signature in black ink, appearing to be a stylized name.



Handwritten signature in black ink, appearing to be a stylized name.

11. MONITORING THE EFFECTIVENESS OF THE STRATEGY

The risk management strategy includes the risk management plans. The Plan is used to monitor the progress of implementing the risk management strategy within the Department. The Risk Management Function within the Department produces quarterly reports on the implementation of risk management, while management reports on their risk management responsibilities reflected in their performance agreements.

Handwritten signatures and initials in black ink, including a large circular mark, a stylized signature, and a small mark resembling a question mark.A handwritten signature in black ink, consisting of a stylized, cursive name.

12. FRAUD PREVENTION AND ANTI-CORRUPTION PLAN

The Department is committed to taking a stand against fraud and corruption, and adopts a ZERO TOLERANCE stance as far as fraud and corruption is concerned. Therefore, the Department has formulated and adopted a Fraud Prevention and Anti-Corruption Policy (separate document).



Handwritten signature in black ink, appearing to be 'S. J. ...'.



Handwritten signature in black ink, appearing to be 'M. ...'.

13. ACCEPTANCE

This risk management strategy is inclusive of the following documentation:

- I. Risk Management Policy and Framework (this document);
- II. Risk Management and Fraud Implementation Plan;
- III. Fraud Prevention and Anti-corruption Policy;
- IV. Fraud & Corruption, Investigation Escalation Policy; and
- V. Whistle Blowing Policy.




EASTERN CAPE DEPARTMENT OF EDUCATION
RISK MANAGEMENT POLICY AND FRAMEWORK

14. RISK MANAGEMENT POLICY AND FRAMEWORK REVIEW:

This Policy and Framework shall be reviewed annually and before the anniversary date as necessary to reflect substantial organisational changes or any change required by law and regulations.

Compiled by:
S.Govind

Reviewed by:



Mr L Njobe
Acting Director: Enterprise Risk And Integrity Management

2020.06.15
Date

Recommended by:



Mr S Ngqwala
Chairperson Risk Committee

2020.06.19
Date

Approved by:



Mr T Kojana:
Accounting Officer
Eastern Cape Department of Education

19/06/2020
Date

