Department of Social Development Enterprise Risk Management Strategy and Implementation Plan 2020/21

Contents

DEPARTMENT OF SOCIAL DEVELOPMENT
ENTERPRISE RISK MANAGEMENT STRATEGY AND IMPLEMENTATION PLAN 2020/21

SECTION 1 - INTRODUCTION

1. BACKGROUND

The Provincial Top Management of the Western Cape Government has adopted the Provincial Enterprise Risk Management Policy and Strategy (PERMPS) on the 25 February 2020. The PERMPS sets out the Province's overall intention in respect to the principles of good enterprise risk management practises. It spells out the objectives of the Provincial Risk management process to ultimately strengthen decision making at various levels of accountability.

The Department furthermore adopted an Enterprise Risk Management Policy on 26 March 2020. This policy articulates the Department's risk management philosophy and captures, on a high-level, the roles and responsibilities of the different role players. It provides the basis for the risk management process in the department which is supplemented with the detail in this strategy.

This ERM strategy and implementation plan outlines how the Department will go about implementing the Enterprise Risk Management Policy adopted by the Accounting Officer. This ERM strategy is informed by the PERMPS, the Department's ERM Policy and the department's risk profile.

2. PURPOSE

The purpose of the ERM strategy and implementation plan is to effect the implementation of risk management in a structured, coherent and systematic manner to:

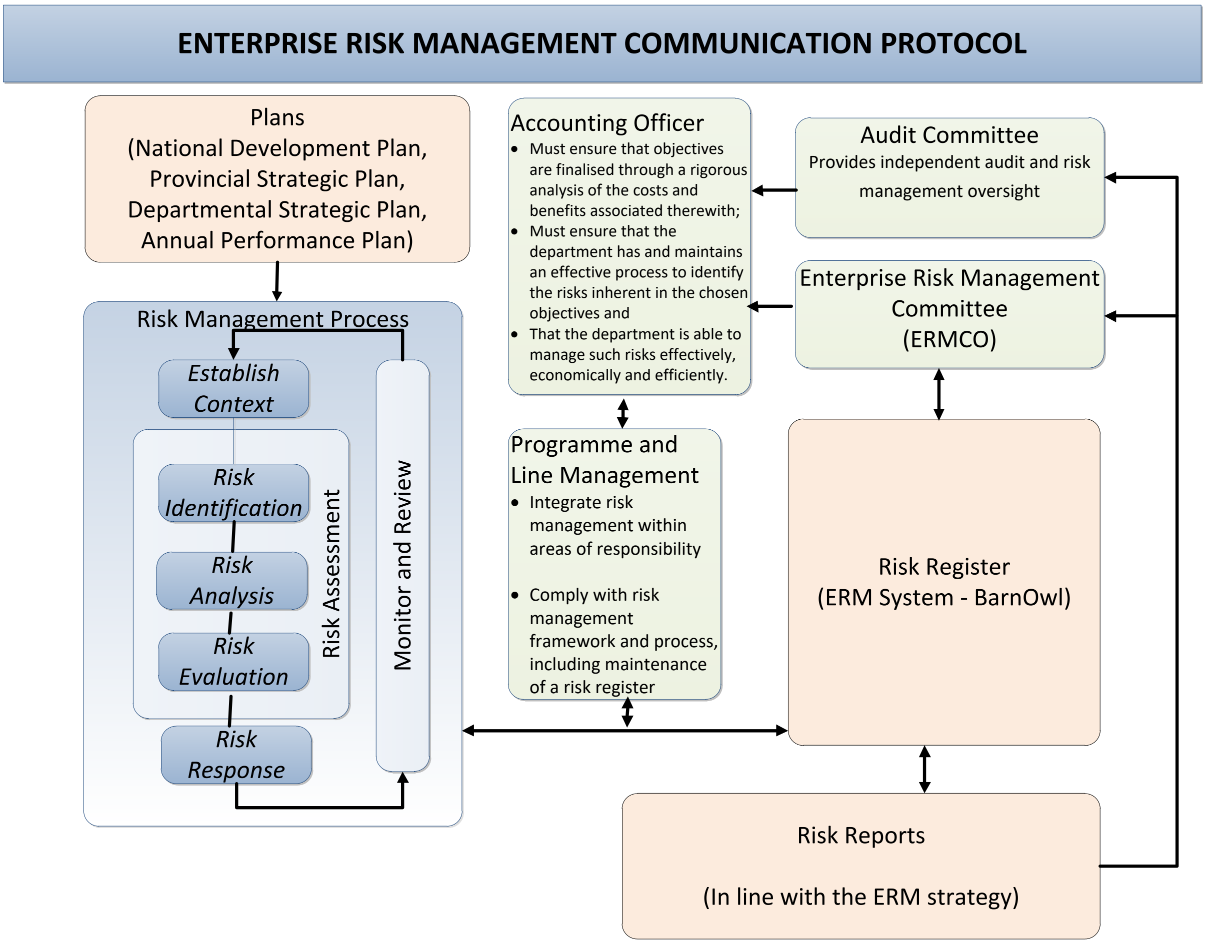
a) ensure that risk management is part of the planning and performance management processes;
b) enable the Department to deliver on the Departmental goals, objectives and targets;
c) improve the quality of decisions and ensure compliance with applicable laws and regulations; and
d) outline and clearly define the roles and responsibilities of managers and staff in embedding risk management in the Department.

It furthermore sets out the risk management activities planned for the 2020/21 financial year.

SECTION 2 – RISK MANAGEMENT PROCESS

Enterprise Risk Management involves the culture, principles, structures and co-ordinated processes and activities to direct and control the effective management of potential (uncertain) opportunities and/or adverse events that a Department may encounter in pursuit of its objective.

The risk management process can be depicted as follows, with each of the steps being described in the rest of this Strategy:



1. ESTABLISHING CONTEXT

By establishing the context, the articulation of objectives, key assumptions, key success factors, key challenges, key changes in the internal and external environment is considered in the risk management process. Context setting sets the scope for identifying risks and opportunities. It sets the boundaries in which risks can be identified and provides relevance for the risk.

2. IDENTIFYING RISKS AND OPPORTUNITIES

Risk identification is a process of finding, recognising and describing risks. The aim of this step is to generate a list of key risks that might impede the achievement of the department's objectives. The focus would therefore be to identify the risks that could prevent achievement of the strategic objectives and key performance indicators of the department, as documented in the Provincial Strategic Plan, and the approved 5-Year Strategic Plan and Annual Performance Plan of the department for the 2020/21 financial year.

When identifying risks, it is essential to align to the outward focussed approach of the Department, thus considering citizen centricity in delivering services. There are various techniques that can be used in the identification of risks and this includes scenario planning, value-chain analysis, causality and PDIA (Problem Driven Iterative Adaptation).

Risks will be identified as follows:

1. Provincial risks –will be risks (positive and negative) that are associated with the implementation of the PSP and the associated VIPs and can be directly linked to matters that could impact citizens. They are of a long term nature (more than 3 years) and require the collaboration at various national and provincial departments and/or forums.
   The following broad criteria will apply:
   - Must impact a number of provincial departments – i.e. could happen in all depts., hence elevated
   - Impact province as a whole (eg changing of provincial boundaries)
   - Risks where treatments are of a transversal nature (i.e. more effective to have a transversal risk treatment – need it in fact to address risk and it is not within a single department's control to address the risk – to reduce the risk must be coordinated on a provincial level)
   - Risks where the "risk owner" is a multidisciplinary team

   Provincial risks will, where relevant, be cascaded down into departments. The major difference between provincial and departmental risks in this case would be that the mitigations for provincial risks will be on a strategy and/or policy level whilst at a departmental level the operationalization of these strategies and/or policies will comprise of the risk mitigations. This of course means that the mitigations implemented and operationalised on a departmental level will have to be considered when provincial risks are assessed. This will ensure a continuous and iterative process of review and alignment.

Provincial risks can also be identified on a departmental level and the process of escalating this to the provincial risk register will happen through the various Lead HOD teams.

2. Strategic risks –affect the department's ability to meet its strategic goals and require oversight by senior executives
   It will include risks that have a transversal impact across the department, impact the vision/goals of the department as recorded in the 5-year Strategic Plan, are of a longer term nature and which are on the Accounting Officer's radar. These risks include the following:
   - Safety of staff delivering services in high risk areas.
   - Inability to effectively address the capacity constraints of NGOs
   - Inadequate human resources (within DSD) to deliver on the departments strategic mandate.
   - Business Continuity/ Disaster Recovery (including pandemic)

3. Programme risks – risks that arise at a programme level. These risks require specific and detailed responses and monitoring regimes. They are short term and linked to the Annual Performance Plan indicators for the specific programme. If not treated and monitored, operational risks could potentially result in major adverse consequences for the department.

Strategic risks will be identified as part of an integrated results-based strategic planning approach. To this end Enterprise Risk Management will form an integral part of strategic planning on a provincial and departmental level to ensure that potential risks are identified as part of the 5-yearly and annual departmental planning processes. For this reason, Enterprise Risk Management will be a critical stakeholder in the departmental planning processes

Strategic risks will be reviewed on an annual basis and Programme risks will be reviewed at minimum on a bi-annual basis, either by means of a self-assessment by the relevant programme manager, or a formal review session facilitated by the Directorate: Enterprise Risk Management. ICT risks will be facilitated by the ICT Governance Team and economic crime risks will be facilitated by the Provincial Forensic Team. Where required other technical experts will be involved.

Apart from formal facilitated sessions, the identification of emerging risks is an important aspect of identifying risks timely and formulating risk response decisions that would minimise the impact and/or likelihood of the risk materialising. To this end, it is required that the Directorate: Enterprise Risk Management be provided with strategic documentation (strategic and annual performance plans, quarterly performance reports, important and relevant functional information, business cases, key strategies, SOP's and policies, etc.) to identify emerging risks for discussion/tabling with management. The strategic documentation is used to prepare for these sessions so that the contribution in these sessions is valuable and strengthen the risk management process.

The identification and discussion of emerging risks will furthermore be included as an agenda item on management meetings. The formal risk assessment process as defined in this ERM Strategy and Implementation Plan will then be followed to analyse and evaluate risks. Risk identification will be included as an agenda point on departmental strategic planning sessions so that Departmental strategies can be evaluated/ considered in light of the risks and opportunities that the Department may be facing.

Risks will be categorised to assist with determining risk owners and risk reporting. The risk categories that will be used for the 2020/21 financial year is attached as **Annexure B**.

3. ANALYSING RISKS

Risk analysis is the process of assessing the inherent and residual risk. The inherent risk assessment establishes the level of exposure in the absence of deliberate management actions to influence the risk. The residual risk assessment determines the actual remaining level of risk after the mitigating effects of management actions to influence the risk. The impact of the potential threat or opportunity, as well as the likelihood of the risk occurring, both inherently and residually is further rated using the matrix in Annexure C.

The risk rating will be determined by multiplying the impact rating with the likelihood rating. The level of risk will be used to depict risks in the risk profile as follows:

Likelihood				
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4
	1	2	3	4

Impact

Range		Level
12 - 16		Extreme
8 - 11		High
3 – 7		Moderate
1 - 2		Low

Ethics risks are the current or potential organisational beliefs, practices, or behaviours (conduct) that either support or are in contravention of organisation-specific standards for desired behaviour, values and/or in contravention of legitimate stakeholder rights and expectations.

Research has shown that most of the contributing factors (causes) of risks are behavioural in nature and this is where ethical risks feature. Some of these ethical risks are already incorporated into the risk profiles of the department. For instance, the contributing factors of economic crime risks are in many instances indicative of lapses in ethical behaviour by employees. Some strategic and operational risks of the department also contain contributing factors that are indicative of lapses in ethical behaviour of employees. It is therefore not necessary at this stage to create a separate risk category for ethical risks

In analysing risks we apply the bow-tie methodology. This methodology provides a structured, systematic way of analysing the risk, by identifying all the contributing factors that could cause a risk to arise and then the associated impacts or consequences should this risk materialise. The ideal is to portray this in an "easy-to-understand" picture which can be used to facilitate the process in a more participative way and to reduce the use of spreadsheets in workshops.

Existing controls (or mitigating measures) and action plans (further controls/mitigations required to adequately mitigate the risk) are identified and linked to each contributing factor and impact. It is possible that a single control or action plan could mitigate multiple contributing factors and/or impacts.

3.1. Identifying contributing factors

To assist in the analysis of risks, contributing factors will be prioritised and categorised to indicate the level of its contribution to the risk. This is to direct attention to identify and/or implement controls that would address the contributing factors that have the highest influence on the risk. This will also assist when risks are rated residually as controls that address a contributing factor that has a low influence on the risk should not result in a significant decrease of the residual risk rating.

Contributing Factor Priorities:

- 1 - Low influence on risk – these are low/ insignificant causes of the risk.
- 2 - Medium influence on risk – these have a moderate/ medium cause to the risk.
- 3 - High influence on risk – these are the highest/ most significant contributors to the risk

Contributing factors will be categorised as either internal or external, with the following sub-categories:

- Internal (People, Process, System)
- External (Economical, Environmental, Legal, Political, Social, Technological)

3.2. Identifying controls

A control is any action taken by management to manage and/or mitigate the risk. A control can be categorised into one of the following categories:

- **Preventative controls** – these controls are designed to limit the possibility of an undesirable outcome being realised. Examples include segregation of duty and limiting levels of authority.

- **Corrective controls** – these controls are designed to correct undesirable outcomes which have been realised (i.e. impact). Example includes design of a contract to allow recovery of overpayments.

- **Directive controls** – these controls are designed to ensure that a particular outcome is achieved and are normally formalised through legislation and/or directives. Example includes a procedure to be followed in an emergency.

- **Detective controls** – these controls are designed to ensure that an undesirable outcome is identified as soon as it occurs in order to control the effect and in order to put measures in place to prevent a re-occurrence. Examples include budget underspending monitoring, stock or asset counts, reconciliations and post implementation reviews.

In identifying controls, it is important that the control that is implemented is proportional to the risk. Every control has an associated cost and it is important that the control action offers value for money in relation to the risk it is controlling. The purpose of controls is to constrain risk rather than to eliminate it.

After controls have been identified, an assessment is performed to determine whether these controls are sufficient to address the risk and whether any control gaps or weaknesses exist in the design of functioning of these controls. Control Self-assessment (CSA) is a process through which the adequacy and effectiveness of controls are examined by management to assess its appropriateness to mitigate the risk to an appropriate level. This evaluation of controls assists risk owners in deriving a more probable risk rating.

Adequacy Assessment

The purpose of this analysis is to determine whether the control design is appropriate, and to identify any potential control gaps or design flaws.

It is important to note the adequacy assessment is performed on the group of controls identified to mitigate the specific contributing factor or impact, not the individual controls. Categories for Adequacy assessments ratings are as follow:

- Adequate;
- Adequate requiring enhancements and
- Inadequate.

Effectiveness assessment

This analysis involves assessing whether the control is consistently applied and whether it is functioning as intended. The effectiveness assessment is performed on each control identified to mitigate the specific contributing factor or impact. Categories for Effectiveness assessment ratings are as follow:

- Effective;
- Partially Effective; and
- Ineffective.

Where any controls are rated other than Adequate and/or Effective, management should identify Action plans, where possible, to address the gap or control weakness, in a means of improving the risk mitigation.

4. EVALUATING RISKS

The evaluation of risks is the process of benchmarking the residual risk against the department's risk appetite and tolerance to determine the need for further management intervention.

4.1. Risk Appetite

Risk appetite provides a boundary around the amount of risk an organization might pursue. An organization with an aggressive appetite for risk might set aggressive goals, while an organisation that is risk-averse, with a low appetite for risk, might set conservative goals. Just as organisations set different objectives, they will develop different risk appetites. There is no standard or universal risk appetite statement that applies to all organisations, nor is there a "right" risk appetite. Management must make choices in setting risk appetite, understanding the trade-offs involved in having higher or lower appetites. A risk appetite statement sets the tone for risk management, a limit beyond which additional risk should not be taken.

Following the direction of the PERMPS, an appetite statement has been defined per risk category to clarify the WCG's and department's appetite for certain categories of risk. This will assist in risk response decisions.

The WCG's risk appetite levels and its associated approach to risks in those levels are depicted as follows:

Risk Appetite Range	**Low**	**Moderate**	**High**
Risk taking vs reward	A cautious approach towards risk taking	A balanced and informed approach to risk taking	Aggressive risk taking is justified
Impact on strategies/	Willing to accept a small negative	Willing to accept some negative	Willing to accept a large negative

objectives	impact in pursuit of strategic objectives	impact in pursuit of strategic objectives	impact in pursuit of strategic objectives
Preferred risk response approach	Risks that cannot be effectively treated or transferred are avoided	No preference towards risk response approaches	Risk is accepted
Risk response decision criteria	Risk response actions are taken even though prevention costs are greater than expected incident costs.	Risk response actions are made based on cost effectiveness, management priorities and potential outcomes.	Minimum, if any, risk response actions are taken

Based on the above, the following risk appetite statements were agreed to by PTM for the WCG and although the Department could be more restrictive in application, it could not relax this overall appetite statement. Decision makers therefore are permitted to expose the WCG to a degree of risk in line with the following appetite statements:

Risk appetite description	Risk appetite statements
Low Appetite	The WCG has a low appetite for non-compliance with legal and regulatory requirements, including deliberate and purposeful violations of legislative and regulatory requirements. We commit to a high level of compliance with relevant legislation, regulation and governance principles where breaches will be remedied as soon as practicable. The WCG has a low appetite for risks relating to economic crime and commits to a zero tolerance for fraud and corruption. We are committed to deter and prevent fraud and corruption, will take a serious approach to cases or suspected cases of fraud and corruption perpetrated by our employees and contractors and will respond fully and fairly in such cases. The WCG has no appetite for fatalities in the workplace and will take the necessary measures to create a safe working environment for our staff after considering all critical areas. We will not allow

Risk appetite description	Risk appetite statements
	behaviour that could harm staff while being at work. The WCG has a low appetite for the compromise of processes governing the use of its information, its management and publication. We commit to ensure that information is authentic, appropriately classified, conserved and managed in accordance with relevant requirements. This further means that we have a low appetite for cyber security risks. The WCG has a low appetite for the loss of fixed, current and moveable assets. The WCG has a low appetite for third party performance and/or contract management risks and will hold all parties/suppliers accountable for contracted services. The WCG has a low appetite for risks that impacts the availability of our systems which supports our core and critical business functions. The WCG has a low appetite for security related risks, including those relating to physical security, access to information and data and cyber security.
Moderate Appetite	The WCG has a moderate appetite for non-compliance with policies and procedures and will ensure that policies and procedures are complied with as far as practicable possible. The WCG has a moderate appetite for risks that may jeopardise its activities and standards of operation and will ensure that it will continue to deliver its services to the people of the Western Cape effectively and efficiently. The WCG has a moderate appetite for risks that can negatively impact on audit outcomes, quality of financial statements, cost structures and financial sustainability, including the SCM process. The WCG has a moderate appetite for risks relating to litigation, penalties, fines and court proceedings. The WCG will exhibit a moderate appetite for risks that affect its reputation. The WCG has a moderate appetite for changes to its culture and leadership. The WCG is building the high-performance, professional and innovative capabilities of its leaders through empowerment and leadership development, within a framework of ethical

Risk appetite description	Risk appetite statements
	behaviour. WCG has a moderate risk appetite to ensure that its workforce is engaged, innovative, future focused and aligned to its strategic priorities and objectives. The WCG focusses on recruiting, retaining and developing a high-quality workforce that reflects the diversity of the RSA. The WCG has a moderate risk appetite for risks that could have an impact on service delivery to the people of the Western Cape and the relevant service delivery indicators. The WCG has a moderate risk appetite for risks associated with infrastructure development, reconstruction and changes to its C-AMP. External risks are those that arise from events outside of the WCG's control. These risks can offer negative and/or positive benefits. The WCG cannot influence the likelihood of these types of risks, but can reduce the cost of an impact. The WCG therefore has a moderate appetite for: • Risks that impact its economic environment including interest rates, exchange rates, share prices, GDP, inflation, employment and investment options. • Risks that impact its legislative sphere. • Challenges faced in the natural environment. • Risks inherent in its political landscape. • Risks emanating from its external social environment (eg urbanisation). • Risks that can negatively impact the WCG's technological environment (advances and changes in technology).
High Appetite	The WCG has a high appetite for excellence and innovation through technology. We acknowledge that digital transformation changes are required to adapt to changes in regulator, society and the general business environment.

For easier reference, the following is a high-level summary of the risk appetite level for each risk category:

LOW APPETITE (risks to be avoided – control systems to be well-designed)	MODERATE APPETITE (conservative risk taking with commensurate control systems)	HIGH APPETITE (receptive to risk-taking within acceptable limits)

Compliance / Regulatory Economic Crime Health and Safety Knowledge and Information Management Loss / Theft of Assets Third party performance / Contract Management Information and Communication Technology (**technology and system uptime**) Security Management	Non-compliance with Policies and Procedures Business Continuity / Disaster Recovery Financial Supply Chain Management Litigation Reputation Organisational Culture People Management Service Delivery Infrastructure development Economic Environment Political Environment Social Environment Natural Environment Technological Environment Legislative Environment	Information and Communication Technology (**digital transformation**)

4.2. Risk Tolerance

The risk tolerance refers to the amount of risk the department is capable of bearing, or the acceptable level of variation relative to achievement of a specific objective, often best measured in the same unit as those used to measure the related objective. It is tactical and operational. Risk tolerance guides operating units as they implement risk appetite and communicates a degree of flexibility. Risk tolerances are a more specific subset of the risk appetite and dissect the assertions that make up the risk appetite statement. Whereas risk appetite is considered in the context of strategic planning and objectives, risk tolerance is considered in developing tactical objectives. That is, it addresses how much deviance from a specific objective the department is willing to allow.

The risk tolerance will be determined per risk, and in line with the abovementioned appetite statements as follows:

- Tolerance level for risks with a low appetite must range from 1 to 4;
- Tolerance level for risks with a moderate appetite must range from 5 to 10; and
- Tolerance level for risks with a high appetite must range from 11 to 16.

4.3. Risk Response Decision

The risk response decision is determined when the residual risk is benchmarked against the agreed tolerance level to determine the need for further management intervention. The risk response categories are the following:

- **Treat/Manage** – the activity or action continues but additional action is necessary to reduce the risk to an acceptable level. The action plans will be formulated as part of the risk evaluation process by providing detail regarding proposed additional actions and/or mitigation strategies which are to be implemented to ensure that the risk is managed down to the desired residual risk rating. The action plans will have action plan owners and due dates recorded and regular follow-ups will take place with the risk owners as to determine progress with implementation. This progress will also be recorded, monitored and reported.

- **Tolerate/Accept** – Where risks are identified as unavoidable or no suitable treatment plans are available or nothing can be done at reasonable costs. The risk should be accepted. This option, of course, may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised and exerting influence as and where required. Tolerating a risk refers to the willingness of the department to live with a risk in order to obtain certain benefits. To tolerate a risk does not mean that the department disregards it.

- **Terminate/Avoid** – This can be done by deciding not to start or continue with a particular activity that gives rise to the risk.

However, the organisational objectives still need to be borne in mind and inappropriate risk aversion may increase other risk areas.

- **Transfer** – This involves other parties bearing or sharing the risk either partially or in full. This may be through contracts, partnerships and/or joint ventures (e.g. Public Private Partnerships).

- **Pending** – emerging risk to still be articulated, assessed and evaluated.

The aforementioned options, will be considered in light of the cost/benefit of implementing the decision. At the same time, the relevant risk appetite statement must be considered, for instance where the statement allows for risk taking, it will not be necessary to design controls for that particular risk

The decision to **Tolerate/ Accept** a risk is taken as follows:

Risk Rating	Decision Authority Level
Green: 2	Directorate and Chief Directorate level
Yellow: 3, 4 or 6	Chief Directorate level
Red: 8, 9, 12 or 16	Departmental EXCO level

Due to the fact that external risks are unavoidable and mostly being tolerated, these risks will in the main be addressed through exerting influence in the relevant structures such as forums/intergovernmental committees.

Some risks arise from events outside the departments/WCG and are beyond our influence or control. External risks therefore require another approach. Because it is not usually within our control to prevent such events from occurring, management must focus on identification and mitigation of their impact. Despite the lack of control over external risks, the department can still manage it by generating ideas about the type and magnitude of external events that could happen, and by developing a plan for mitigating the negative impact if such an event actually materialises.

5. OTHER MATTERS

5.1. Assurance Providers

The Combined Assurance Framework for the WCG (adopted by PTM during March 2015) is an important part of the WCG's overall risk management and governance framework. The ultimate purpose of the Framework is to be a strategic management tool that facilitates the decision-making process relating to the coordination and integration of assurance efforts, ensuring optimal coverage of risks facing the WCG. The assessment of the risks facing the WCG, control mitigations in place and the assurances received by management form the basis for this Framework.
The WCG Combined Assurance Framework defines three levels of assurance:

1. **Management assurance** which is the first level of assurance that line management provide relating to managing risks. Line management is responsible for maintaining effective internal controls and executing control procedures on a day-to-day basis. Line management is responsible for ensuring that adequate supervisory controls are in place to ensure compliance to control measures and to highlight control breakdowns, inadequate processes and unexpected events, and take the required remedial action. The framework further stipulates that management monitoring meetings, supervisory/monitoring control mechanisms, strategy implementation monitoring and management assessments are considered to be "management assurance".
2. **Internal assurance** is the second level of assurance that is provided by functions separate and independent from direct line management entrusted with assessing adherence to policies and procedures, norms and standards and/or frameworks. This includes work performed by Internal Control Units, Monitoring and Evaluation units, Technical Quality Assurance units and Provincial Treasury.
3. **Independent assurance** is the third level of assurance provided by functions that are guided by professional standards requiring the highest levels of independence. These include the Auditor General of South African and the WCG Internal Audit Function.

5.2. Risk profile

The outcome of the risk assessment process is a risk profile. The department will use the risk profile as key driver toward integrating risk management in the strategic planning process and ensuring that the risk profile is used as an underpinning resource to assist in strategic planning, setting priorities and resource allocation. Refer to the department's detailed risk register and risk profiles presented in the quarter three Audit Committee of 14 February 2019.

5.3. Risk Management Information System

BarnOwl is the Risk Management Information System. Risk information is captured on BarnOwl and the results are distributed to the programme managers by e-mail. Programme managers are expected to approve the risk registers subsequent to risk assessment workshops using the voting buttons provided in the e-mail they will receive or by return e-mail where relevant. This electronic approval will be safeguarded on BarnOwl as proof that the registers were indeed approved.

Due to a limited number of licences available, access to BarnOwl is restricted to the Chief Risk Officer responsible for the Department (currently Steven Africa), the IT Governance Office and Provincial Forensic Services. Risk information is readily available and can be customised according to the needs of the department.

6. RISK REPORTING PROCESS

6.1. The results of the programme engagements form the basis of a presentation that will be prepared for the Enterprise Risk Management Committee. The approved Terms of Reference of the Enterprise Risk Management Committee depicts the responsibility of the Committee as it relates to Enterprise Risk Management. The following will be focussed on as it relates to the individual risks:

a. Risks outside the agreed tolerance levels to assess the mitigating strategies in place and recommend any additional actions that could further reduce the residual risk rating;
b. Risks tolerated by the respective risk owners to ensure that the risks indeed are unavoidable or that no suitable treatment plans are available at a reasonable cost to further reduce the residual risk rating;
c. Risks below the agreed tolerance levels will be reviewed on a high level to ensure that they are adequately managed by the risk owners.
d. Status of implementation of agreed action plans.

6.2. The quarterly report to the relevant Audit Committee will be used by the Audit Committee to execute its oversight function relating to risk management as documented in the approved Terms of Reference of Audit Committees. Where required, the Audit Committee will make recommendations to the Accounting Officer for consideration in improving the risk management process.

6.3. External communication of risks are limited to the risks and mitigation actions recorded in the approved Annual Performance Plan of the Department.

6.4. Where relevant, other organs of state will be engaged in instances where their participation is required in the management of a particular risk.

7. RISK REPORTS

The following reports will be delivered:

7.1. The Directorate: Enterprise Risk Management (D: ERM) will prepare a quarterly report to the Head of the Department and Chairperson of the relevant Audit Committee. This report will contain the following:
  a. Executive Summary
  b. A status report on the progress made against the approved ERM Implementation Plan (by both D: ERM and the Department);
  c. Deliberations at GOVCOM, focussing on the risks that are outside the agreed tolerance level and subsequent resolution;
  d. Status of implementation of action plans agreed to;
  e. The final risk registers and profiles (for all programmes);
  f. Top five Strategic risks of the Department
  g. Risks to be escalated to Provincial risk register, if any; and
  h. Movement in residual ratings of strategic risks; and
  i. Present any relevant risk management information / intelligence.

7.2. D: ERM will submit the second quarter risk registers and profiles to the Department's Internal Audit team to inform the Internal Audit Plans of the Department.

7.3. D: ERM will submit relevant risk information to the Auditor-General of South Africa during their annual audit process upon receipt of a Request For Information (RFI).

7.4. D: ERM will submit input for Part C: Governance of the Annual Report to the Accounting Officer.

7.5. Should risk-related information be requested by any other party (other than officials in the department, the Audit Committee and Internal Audit, AGSA), the request will be consulted with the Head of the Department in collaboration with the departmental Security Manager prior to information being provided.

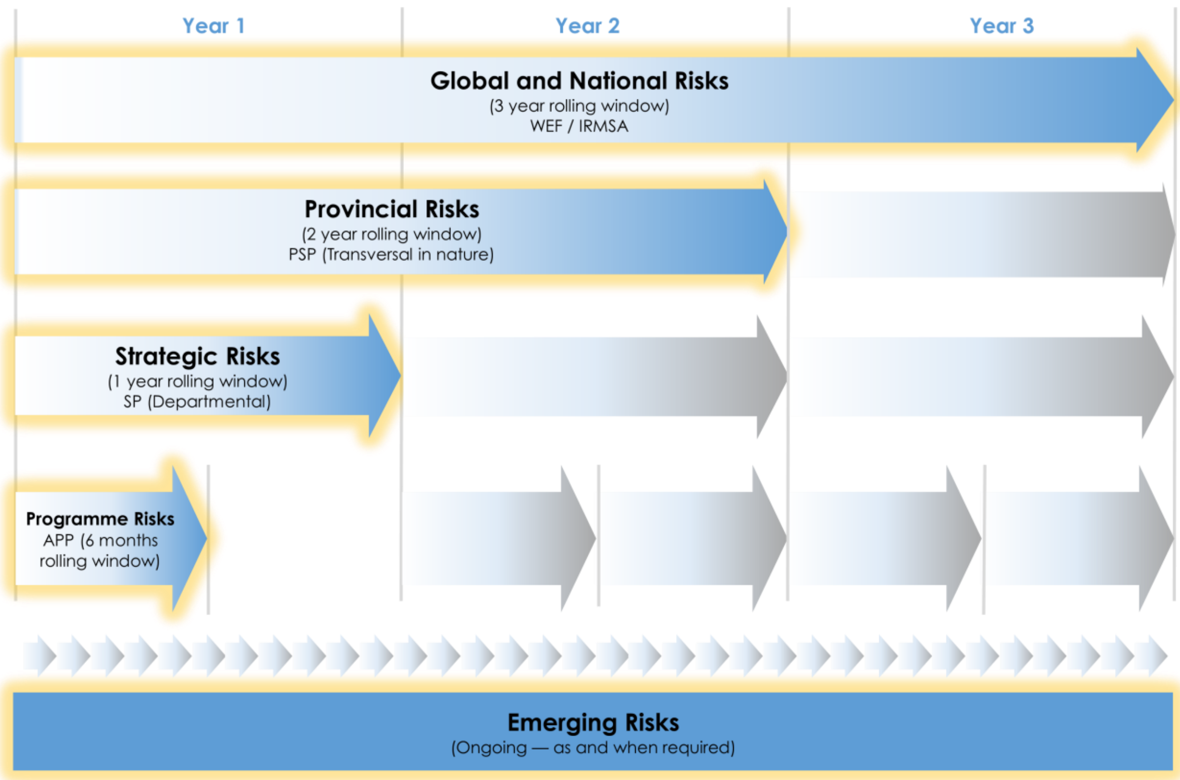
7.6. The Risk Management Information System is hosted by D: ERM. The department can at any time request additional reports/information from the system and this will be made available to the department.

8. MONITORING

The evaluation of risk management effectiveness is vital to maximise the value created through the risk management practice. Risk management should be regularly monitored through a process that assesses both the presence and functioning of its components and the quality of the Department's performance over time. Monitoring can be done through ongoing activities, independent evaluations and self-assessments.

8.1. Ongoing Activities

a) A regular review of the risks, controls and action plans are essential to determine if the processes implemented to treat the risks are adequate and effective. At a management level this process will be effected at yearly risk assessment sessions (strategic risks) and bi-annual (programme risks) Risk Assessment sessions of the Department and its programmes. Feedback received in terms of adequacy of the treatments enables the organisation to analyse and learn from success, failures and near-misses.



Risks emanating from the World Economic Forum, IRMSA and other global report risks will be reviewed every 3 years. Risks relating to the PSP and

VIPs will be reviewed every two years.

b) The Department will link risks to the Annual Performance Plan (APP) and operational plans of the Department on all levels as a strategy to ensure the integration of risk management into its organisational activities. In this process, the Department will engage with D: ERM to ensure that the risk profile of the Department is taken into account.

c) ERMCO will evaluate the extent and effectiveness of integrating risk management within the Department as part of their responsibilities.

8.2. Independent Evaluations

a) The role of Internal Audit in risk management is to provide an independent, objective assurance on the effectiveness of the department's system of risk management. The results of the internal audits evaluations are incorporated into the departments risk register in respect of risk enhancements. Internal Audit must evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary. This will be considered in line with the risk profile of each department at the time of planning the internal audit coverage for the department.

b) The risk maturity will be assessed as part of the corporate governance maturity baseline assessment is still a work in progress as part of the 2019/20 assessment.

c) The role of the Auditor-General of South Africa is to review the risk management process to ensure it complies with the requirements of section 38(1)(a)(i) of the Public Finance Management Act. They furthermore consider risks during the strategic and detailed planning processes of the regularity audit.

9. ROLES AND RESPONSIBILITIES

The high-level roles and responsibilities of all role players are as per the approved ERM Policy of the Department. This is augmented by the detail contained in the National Treasury Public Sector Risk Management Framework.

The risk champion of the Department of Social Development is Mr Juan Smith. The Chief Risk officer responsibility is executed by the Directorate: Enterprise Risk

Management in the Department of the Premier. The specific person allocated to the is Mr Steven Africa.

10. TRAINING AND AWARENESS

It is essential that all Departmental managers and other key personnel involved in the risk management process are well trained in risk management methodologies and approaches. The training and awareness programme to be rolled out to the Department for 2020/21 includes the following:

- The approved ERM Policy and ERM Strategy and Implementation Plan for 2020/21 will be distributed to all employees through the departmental communications channels. These two documents will furthermore be safeguarded on the departmental shared drive for access by all employees;
- Risk awareness sessions to be conducted by D: ERM to officials as agreed with the Department. Relevant contents from the ERM Policy and ERM Strategy and Implementation Plan for 2020/21 will be included in these awareness sessions.

11. BUSINESS CONTINUITY

Business Continuity Management entails the Department's ability to ensure critical business functions will continue to operate despite serious incidents or disasters that might otherwise have interrupted these critical functions, the department's ability to recover operationally within a reasonably short period.

The Department has developed a Business Continuity Plan for six critical departmental functions. These include functions related to Centre for e-Innovation, Secretariat Services, Supply Chain Management and Administration, Financial Management, Service Benefits, and Recruitment and Selection. In addition, the Centre for e-Innovation advanced with the development of a disaster recovery plan as well as the identification of key personnel in cases of emergencies. The implementation of the Business Continuity Plan will be monitored on a quarterly basis by ERMCO.

12. FRAUD PREVENTION PLAN

The Department has a detailed approved Fraud and Corruption Prevention Plan together with an Implementation Plan that expires on 31 March 2022.

13. ERM IMPLEMENTATION PLAN

The ERM Implementation Plan for the Department was prepared to give effect to the ERM Policy and Strategy and sets out the activities planned for the 2020/21 financial year. It considered:

- The risk management policy;
- The risk management strategy;
- Available resources; and
- Quick wins and sustainability.

The detailed ERM Implementation Plan is included as **Annexure D**.

14. CONCLUSION

a) The Enterprise Risk Management Strategy and Implementation Plan for 2020/21 takes into consideration the current state versus the desired state in order to progressively move toward a risk mature and risk intelligent organisation.
b) This document will be reviewed on an annual basis to ensure that it remains relevant to the department's needs and any amendments will be communicated to all relevant stakeholders.

Recommended by the Economic Cluster Audit Committee:

___electronically signed__

Mr. A. Amod,

Chairperson of the Audit Committee

Date: 26 March 2020

Approved by the Accounting Officer:

Dr. R. Macdonald

Signature: ______________________

Date: ______________________

ANNEXURE A: GLOSSARY OF TERMS

GLOSSARY OF TERMS

Term	Definition/Meaning
Action Plans	Actions to be implemented by management to further manage (mitigate) and reduce the level of risk.
Business Continuity	Creating the ability to continue delivery of services at acceptable levels following a disruptive event (materialization of a risk)
Business Continuity Plan	The documented procedures that guide the ability to respond, recover, resume and restore services following a disruption
Consequence	Outcome of an actual event (i.e. after risk materialized) impacting on the department's objectives.
Control	Any action taken to manage risk.
Control Owner	The person responsible for executing the control.
Impact	The potential seriousness should a risk materialise.
Inherent Risk	The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.
Likelihood	The chance of something happening.
Opportunity	The positive consequence resulting from the adequate treatment of a risk or event or in pursuit of objectives.
Programme Risk	Those risks that arise at a programme level. These risks require specific and detailed responses and monitoring regimes. They are short term and linked to the Annual Performance Plan indicators for the specific programme. If not treated and monitored, operational risks could potentially result in major adverse consequences for the Department
Residual Risk	The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk).
Risk	An unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities.
Risk Aggregation	Risk aggregation is the "roll-up" of low level risks to higher levels (i.e. risks on a project level represented on a departmental level).
Risk Appetite	The risk appetite is the amount of risk, on a broad level, a department is willing to accept in pursuit of value. It reflects the department's risk management philosophy, and in turn influences the department's culture and operating style and guides resource allocation. It aligns the organisation, people and processes necessary to respond to and monitor risk. It sets a limit beyond which additional risk should not be taken.
Risk Assessment	**Risk Assessment:** the overall process of risk identification, risk analysis and risk evaluation: - **Risk Identification:** the process of identifying, recognising and describing risks. - **Risk Analysis:** the process of assessing the inherent risk to establish the

Term	Definition/Meaning
	level of exposure in the absence of deliberate management actions to influence the risk and the process of assessing the residual risk to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk. - **Risk Evaluation:** the process of benchmarking the residual risk against the department's risk appetite to determine the need for further management intervention.
Risk Champion	A person who, by virtue of his/her expertise or authority, champions a particular aspect of the risk management process, but who is not the risk owner.
Risk Criteria	The terms against which the significance of a risk is evaluated (i.e. risk appetite and tolerance levels).
Risk Factor	Any threat or event which creates, or has the potential to create risk. This is also referred to as "Contributing Factors".
Risk Management	A systematic and formalised process to assess, manage and monitor risks.
Risk Management Committee	A committee appointed by the Accounting Officer / Authority to review the Institution's system of risk management.
Risk Management Framework	The set of components providing the foundation for risk management within the department. It consists of: - The Department's Risk Management Policy; - The Department's Risk Management Strategy; and - The Department's Risk Management Implementation Plan.
Risk Management Implementation Plan	The plan that facilitates the execution of risk management in a department. It gives effect to the department's risk management policy and strategy and contains the activities, responsibilities and resources to be applied to the management of risk.
Risk Management Unit	A business unit responsible for coordinating and supporting the overall departmental risk management process, but which does not assume the responsibilities of Management for identifying, assessing and managing risk. This responsibility currently resides in the Directorate: Enterprise Risk Management in the Department of the Premier.
Risk Owner	The person accountable for managing a particular risk.
Risk Profile (Heatmap)	The documented and prioritised overall assessment of a range of specific risks faced by the department.
Risk Rating	The rating resulting from the application of the department's risk analysis matrix by multiplying the likelihood and impact ratings.
Risk Register	Record of information about identified and assessed risks.
Risk Management Strategy	Records the process of implementing the department's risk management policy, as approved by the Accounting Officer.
Risk Management Policy	Communicates the department's risk management philosophy in the context of how risk management is expected to support the department in achieving its objectives.
Risk Tolerance	The risk tolerance refers to the amount of risk the department is capable of bearing, or the acceptable level of variation relative to achievement of a specific objective, often best measured in same unit as those used to measure the related objective. It is tactical and operational. Risk

Term	Definition/Meaning
	tolerances guide operating units as they implement risk appetite and communicates a degree of flexibility. Risk tolerances are a more specific subset of the risk appetite and dissect the assertions that make up the risk appetite statement. Whereas risk appetite is considered in the context of strategic planning and objectives, risk tolerance is considered in developing tactical objectives. That is, it addresses how much deviance from a specific objective the department is willing to allow.
Strategic Risk	Risks that affect the department's ability to meet its strategic goals and require oversight by senior executives. It relates to risks that have a departmental transversal impact, risks that impact the vision/goals of the department as recorded in its 5-year strategic plan, are of a longer term nature and which are on the radar of the Accounting Officer.

ANNEXURE B: RISK CATEGORIES

RISK CATEGORIES

The main categories to group individual risks will be the following:

RISK TYPE	RISK CATEGORY	DESCRIPTION
Internal	People Management	Risks that relate to human resources of the department. These risks can have an effect on a department's human capital with regard to: • Integrity and honesty; • Recruitment; • Skills and competence; • Employee wellness; • Employee relations; • Retention; etc
	Knowledge and Information management	Risks relating to the department's management of knowledge and information. The following aspects related to knowledge management are included: • Availability of information; • Stability of the information; • Integrity of information data; • Relevance of the information; • Retention; and • Safeguarding.
	Litigation	Risks that the department might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: • Claims by employees, the public, service providers and other third parties; and • Failure by the department to exercise certain rights that are to its advantage.
	Loss/theft of assets	Risks that the department might suffer losses due to either theft or loss of an asset of the department.
	Supply Chain Management	Risks relating to the department's supply chain. Possible aspects to consider include: • Availability of material; • Costs and means of acquiring \ procuring resources; and • The wastage of material resources.
	Service delivery	Every department exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the citizens.

RISK TYPE	RISK CATEGORY	DESCRIPTION
	Information and Communication Technology	The risks relating specifically to the department's ICT objectives, infrastructure requirement, etc. Possible considerations could include the following: • Security concerns; including Cyber-security • Technology availability (uptime); • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology.
	Third party performance/ Contract management	Risks related to the department's dependence on the performance of a third party. Non-performance could include: • Outright failure to perform; • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
	Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the department.
	Business Continuity/Disaster Recovery	Risks related to the department's preparedness or absence thereto to disasters that could impact the normal functioning of the Institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: • Disaster management procedures; and • Contingency planning.

RISK TYPE	RISK CATEGORY	DESCRIPTION
	Compliance/Regulatory	Risks related to the compliance requirements that the department has to meet. Aspects to consider in this regard are: • Failure to monitor or enforce compliance • Monitoring and enforcement mechanisms; • Consequences of non-compliance; and • Fines and penalties.
	Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the department's assets or resources.
	Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: • Cash flow adequacy and management thereof; • Financial losses; • Wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and • Increasing operational expenditure.
	Organisational Culture	Risks relating to the department's overall culture and control environment. The various factors related to organisational culture include: • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management style.
	Reputation	Factors that could result in the tarnishing of the department's reputation, public perception and image.
	Security Management	Factors to consider include: • Document classification and security; • Physical security; and • Personnel security (vetting).

RISK TYPE	RISK CATEGORY	DESCRIPTION
External	Economic Environment	Risks related to the department's economic environment. Factors to consider include: • Inflation; • Foreign exchange fluctuations; and • Interest rates.
	Political environment	Risks emanating from political factors and decisions that have an impact on the department's mandate and operations. Possible factors to consider include: • Political unrest; • Local, Provincial and National elections; and • Changes in office bearers.
	Social environment	Risks related to the department's social environment. Possible factors to consider include: • Unemployment; and • Migration of workers.
	Natural environment	Risks relating to the department's natural environment and its impact on normal operations. Consider factors such as: • Depletion of natural resources; • Environmental degradation; • Spillage; and • Pollution.
	Technological environment	Risks emanating from the effects of advancements and changes in technology.
	Legislative environment	Risks related to the department's legislative environment e.g. changes in legislation, conflicting legislation.

ANNEXURE C: RISK ANALYSIS (IMPACT & LIKELIHOOD)

Category/Domain	1	2	3	4
	Low	Moderate	High	Extreme
Service Delivery	Minor impact on front line service delivery Performance indicators and targets will still be achieved	Noticeable impact on front line service delivery Achievement of performance indicators and targets is at risk	Major impact on front line service delivery <15% negative variance on achievement of performance indicators and targets Key objective not met	Critical, long term impact on front line service delivery >15% negative variance on achievement of performance indicators and targets Key objective not met
People Management	Staffing levels temporarily reduces service quality	Late delivery of key objectives/ services due to a lack of staff Low staff morale	Uncertain delivery of key objectives/ services due to a lack of staff Loss of key staff Very low staff morale	Non-delivery of key objectives/ services due to a lack of staff Loss of several key staff
Financial	Underspending budget by x% Irregular expenditure of Rxx Fruitless and wasteful expenditure of Rx	Underspending budget by x% Irregular expenditure of Rxx Fruitless and wasteful expenditure of Rx	Underspending budget by x% Irregular expenditure of Rxx Fruitless and wasteful expenditure of Rx	Underspending budget by x% Irregular expenditure of Rxx Fruitless and wasteful expenditure of Rx
Economic Crime	Risk factor has little to no ability to independently cause damage to the department's financial, operational, reputational	Risk factor has below average ability to independently cause damage to the department's financial, operational, reputational and regulatory status	Risk factor can independently cause considerable damage to the department's financial, operational, reputational and regulatory	Risk factor can independently cause devastating damage to the department's financial, operational, reputational and regulatory

Category/Domain	1	2	3	4
	Low	Moderate	High	Extreme
	and regulatory status		status	status
Compliance	No or minimal impact or breach of statutory duty	Single breach in statutory duty Challenging external recommendations	Multiple breaches in statutory duty Critical report	Breaches that could result in legal action / prosecution Severely critical report
Reputation	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence.	National media coverage with service well below reasonable public expectation	National media coverage Total loss of public confidence
Environmental impact	Minor impact on environment	Moderate impact on environment	Major impact on environment	Catastrophic impact on environment
Economic Environment	Minor impact on the economy	Moderate impact on the economy	Major impact on the economy	Catastrophic impact on the economy
Safety and Security	Minor injury or illness requiring minor intervention	Moderate injury requiring professional intervention	Major injury leading to long-term incapacity / disability	Incident leading to death An event impacting on a large number of staff
Organisational Culture	Employees values (that are driven by their actions and behaviours are mostly aligned to the organisational values. There are low	Employee's values are moderately aligned to the organisational values. Moderate level of cultural entropy experienced (21-30%) There are	Employee's values are highly miss aligned to the organisations values. There are high level of cultural entropy experienced	Employee's values are critically miss aligned to the organisations values. There are extremely high levels of cultural entropy

Category/Domain	1	2	3	4
	Low	**Moderate**	**High**	**Extreme**
	levels of cultural entropy experienced (10-20%) There are some problems requiring careful monitoring.	significant problems requiring attention	(31-40%) This is a serious situation requiring immediate leadership intervention and changes.	experienced (Above 41%). This is a critical situation requiring leadership changes since the organisation as a whole could fail if not addressed.
Business Continuity Management /Disaster Recovery	Non-availability of IT Services(s) supporting critical business processes less than defined Recovery Time Objective Electronic Information recoverable within recovery Point Objective	Non availability of IT Service(s) supporting critical business processes with moderate likelihood of exceeding defined RTO (can be mitigated by testing) Electronic Information recoverable within Recovery Point Objective	Non availability of IT Service(s) supporting critical business processes with high likelihood of exceeding RTO Electronic Information recoverable outside Recovery Point Objective (loss of critical data)	Non availability of IT Service (s) supporting critical business processes with certain likelihood exceeding RTO Information unrecoverable
Information Communication and Technology	Enhancements to multiple critical systems to improve functionality and sustain service delivery where necessary All worthwhile technologies exploited and adopted where	Moderate enhancements to critical systems that require improvements to multiple critical systems Adequate technologies exploited and adopted Appropriate interoperability of	Limited enhancements to critical systems in dire need of enhancements to improve service delivery Very limited technologies exploited and adopted where necessary	No new technologies exploited and adopted No operability of critical systems and technologies exist. Sioled operations without capability of

Category/Domain	1	2	3	4
	Low	**Moderate**	**High**	**Extreme**
	necessary Fully operable systems and technologies across the entire organisation	systems and technologies across core business units	Limited operability of systems and technologies, pockets of silos exist within same business unit	interoperability
General	Negative outcomes or missed opportunities that are likely to have a negligible impact on the ability to meet objectives. Event will be controlled through normal management processes.	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives. Event resulting in breakdown of core business process activity.	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives. Event resulting in breakdown of core business process.	Negative outcomes or missed opportunities that are of critical importance to the achievement of the objectives. Critical event resulting in breakdown of core business service.

Likelihood	1	2	3	4
	Unlikely	**Moderate**	**Likely**	**Almost Certain**
Frequency	Highly unlikely that the adverse event/opportunity will occur (0 – 20% likelihood of occurring). The adverse event/opportunity occurs infrequently and is unlikely to occur in the next 5 years.	Unlikely but there is a possibility that the adverse event/opportunity will occur (21 - 50% likelihood of occurring). There is an above average chance that the adverse event/opportunity will occur at least once in the next 36 – 60 months.	Likely that the adverse event/opportunity will occur (51 – 80% likelihood of occurring). History of occurrence internally or at similar institution. It is likely to occur in the next 12 – 36 months.	Adverse event/ opportunity will definitely occur (more than 80% likelihood of occurring). It is likely to occur more than once in the next 12 months.

ANNEXURE D: ERM IMPLEMENTATION PLAN

No	Activity	Output	Due Date	Responsible Person
1	**Risk Governance**			
1.1	Develop and approve Departmental ERM Policy	Approved ERM Policy for 2020/25	30 April 2020	Accounting Officer with assistance from D: ERM
		Publicise (on Departmental Intranet) and communicate contents of ERM Policy to all officials	31 May 2020	Accounting Officer with assistance from D: ERM
1.2	Develop and approve Departmental ERM Strategy and Implementation Plan for next financial year	Approved ERM Strategy and Implementation plan for 2021/22	30 April 2021	Accounting Officer with assistance from D: ERM
		Publicise (on Departmental Intranet) and communicate contents of ERM Strategy and Implementation Plan to all officials	31 May 2021	Accounting Officer with assistance from D: ERM
1.3	Implementation of the Fraud and Corruption and Prevention and Response Plan	Approved Fraud and Corruption Prevention and Response Implementation plan	31 March 2019	Accounting Officer with assistance from PFS
		Completed activities for 2020/21 as per the approved Fraud and Corruption Prevention and Response Implementation plan	31 March 2021	Accounting Officer with assistance from PFS
		Quarterly feedback at ERMCO's re status of implementation of Fraud and Corruption Prevention and Response Implementation Plan	At quarterly ERMCO's	PFS for actions allocated to PFS and Accounting Officer for actions allocated to Department
1.4	Implementation of Business Continuity Plan	Quarterly feedback at ERMCO's re status of implementation of Business Continuity Plan	At quarterly ERMCO's	Accounting Officer

No	Activity	Output	Due Date	Responsible Person
1.5	Active ERMCO with approved Terms of Reference	ERMCO Terms of Reference	Approved on 14 February 2019, will be reviewed when necessary.	Accounting Officer with assistance from D: ERM
		Member appointment letters	31 March 2020	Accounting Officer with assistance from D: ERM
		Quarterly ERMCO's with relevant agenda's attended by all relevant risk practitioners	Quarterly	Accounting Officer
1.6	Assign Risk Champion for next financial year	Confirmation of Risk Champion	31 March 2020	Accounting Officer
1.7	Further embedding risk management in the department to make it part of decision-making and the culture	Management meetings to include an agenda point on risk management where emerging risks are identified and discussed and escalated for detailed risk assessment	Ongoing	Accounting Officer
2	**Risk Identification, Analysis and Evaluation**			
2.1	Annual review and approval of the Strategic Risk Register	1 Strategic Risk Register approved by the Accounting Officer	31 March 2021	Accounting Officer with assistance from D: ERM
2.2	Bi-annual review and approval of the Programme Risk Register	2 Programme Risk Registers approved by the respective Programme Manager for the following programmes: a) Programme 1: Administration b) Programme 2: Social Services c) Programme 3: Children and Families d) Programme 4: Restorative Services	30 September 2020 and 31 March 2021	Programme Managers with assistance from D: ERM

No	Activity	Output	Due Date	Responsible Person
		e) Programme 5: Development and Research f) A Regional Risk Register consolidated for all regions		
2.3	Risk Intelligence	2 trend reports extracted from BarnOwl and/or research used to improve risk discussions.	31 March 2021	D:ERM
2.4	Enable citizen centric approach during the identification of risks, ensuring that the causes and impacts of the risk are assessed with a citizen perspective	45% of risks identified are citizen centric	31 March 2021	Programme Managers with assistance from D: ERM
3	**Risk Reporting**			
3.1	Prepare and deliver agreed reports	Quarterly report to Head of the Department	15 July 2020 15 October 2020 15 January 2021 15 April 2021	D: ERM
		Quarterly report to Audit Committee	31 July 2020 30 October 2020 29 January 2021 30 April 2021	D: ERM
		Second quarter risk register and profile to Internal Audit	15 October 2020	D: ERM
		Submission of relevant risk information to AGSA during their annual audit process	As required by AGSA	D: ERM
		Relevant risk management input into Part C: Governance of the 2019/20 Annual Report	May 2020	D: ERM
4	**Risk Monitoring**			
4.2	Considering of risks during strategic	Risks incorporated into Department's APP for	28 February 2021	Programme Managers

No	Activity	Output	Due Date	Responsible Person
	planning of the Department	2021/22		
5	**Risk Awareness and Training**			
5.1	Present risk awareness sessions	2 Risk Awareness Sessions facilitated by D: ERM	31 March 2021	D: ERM